



## **GLOBALCONNECT A/S**

**INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT FOR THE PERIOD FROM 1 JANUARY TO 31 DECEMBER 2019 ON THE DESCRIPTION OF GLOBALCONNECT OUTSOURCING SERVICES AND THE RELATED TECHNICAL AND ORGANISATIONAL MEASURES AND OTHER CONTROLS AND THEIR DESIGN AND OPERATING EFFECTIVENESS, RELATING TO PROCESSING AND PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE EU GENERAL DATA PROTECTION REGULATION AND THE DANISH ACT ON SUPPLEMENTARY PROVISIONS**

## CONTENTS

<b>INDEPENDENT AUDITOR'S REPORT .....</b>	<b>2</b>
<b>GLOBALCONNECT A/S' STATEMENT .....</b>	<b>5</b>
<b>GLOBALCONNECT A/S' DESCRIPTION OF GLOBALCONNECT OUTSOURCING SERVICES .....</b>	<b>7</b>
General description of GlobalConnect .....	7
Description of GlobalConnect Outsourcing Services' and processing of personal data.....	7
General description of GlobalConnect Outsourcing Services' organisation .....	8
Management of personal data security .....	8
Risk management of GlobalConnect Outsourcing Services .....	10
Control framework, control structure and criteria for control implementation .....	10
Changes to services and relating controls .....	19
Supplementary information on the implemented control environment .....	19
<b>CONTROL OBJECTIVES, CONTROL ACTIVITIES, TESTS AND RESULT OF TESTS .....</b>	<b>20</b>
Risk assessment .....	22
A.5: Information security policies .....	23
A.6: Organisation of information security .....	25
A.7: Human resource security .....	27
A.8: Asset management .....	31
A.9: Access management .....	33
A.10: Cryptography .....	36
A.11: Physical and environmental security .....	37
A.12: Operations security .....	39
A.13: Communications security .....	44
A.14: System acquisition, development and maintenance of systems .....	45
A.15: Supplier relationships .....	47
A.16: Information security incident management .....	49
A.17: Information security aspects of disaster recovery, contingency and restore management .....	52
A.18: Compliance .....	53
<b>SUPPLEMENTARY INFORMATION FROM GLOBALCONNECT A/S .....</b>	<b>57</b>

## INDEPENDENT AUDITOR'S REPORT

**INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT FOR THE PERIOD FROM 1 JANUARY TO 31 DECEMBER 2019 ON THE DESCRIPTION OF GLOBALCONNECT OUTSOURCING SERVICES AND RELATED TECHNICAL AND ORGANISATIONAL MEASURES AND OTHER CONTROLS AND THEIR DESIGN AND OPERATING EFFECTIVENESS, RELATING TO PROCESSING AND PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE EU GENERAL DATA PROTECTION REGULATION AND THE DANISH ACT ON SUPPLEMENTARY PROVISIONS**

To: The Management of GlobalConnect A/S  
GlobalConnect A/S' Customers (Controllers)

### Scope

We were engaged to report on GlobalConnect A/S' (Data Processor) description at pages 7 to 19 of GlobalConnect Outsourcing Services and the related technical and organisational measures and other controls, relating to processing and protection of personal data in accordance with the Regulation of the European Parliament and of the Council on protection of natural persons with regard to processing of personal data and on the free movement of such data (EU General Data Protection Regulation) and the Danish Act on Supplementary Provisions to the Regulation (Danish Data Protection Act), and on the design and operating effectiveness of the technical and organisational measures and other controls relating to the control objectives stated in the description, throughout the period from 1 January to 31 December 2019.

### Data Processor's Responsibilities

The Data Processor is responsible for preparing the statement at page 5 to 6 and the accompanying description including the completeness, accuracy, and method of presenting the statement and the description. Furthermore, the Processor is responsible for providing the services covered by the description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

### Auditor's Independence and Quality Control

We have complied with the independence and other ethical requirements according to the international ethical rules applying to accountants (IESBA's Ethical Rules), which are based on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional conduct.

We are subject to the international standard on quality control, ISQC 1, and accordingly use and maintain a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

### Auditor's Responsibilities

Our responsibility is to express an opinion on the Processor's description and on the design and operating effectiveness of the controls related to the control objectives stated in the description, based on our procedures.

We conducted our engagement in accordance with the International Standard on Assurance Engagements 3000, "Assurance Reports Other Than Audits or Reviews of Historical Financial Information". That standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are appropriately designed and operating effectively.

An assurance engagement to report on the description, design, and operating effectiveness of controls at a data processor involves performing procedures to obtain evidence about the disclosures in the data processor's description and about the design and operating effectiveness of the controls. The procedures selected depend on the auditor's judgment, including the assessment of the risks that the description is not fairly presented, and that controls are not appropriately designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the appropriateness of the objectives stated therein, and the appropriateness of the criteria specified by the data processor and described on page 5 to 6.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

### **Limitations of Controls at a Data Processor**

The Data Processor's Description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of the use of GlobalConnect Outsourcing Services, that the individual data controllers may consider important in their particular circumstances. Also, because of their nature, controls at a data processor may not prevent or detect personal data breaches. Furthermore, the projection of any evaluation of the operating effectiveness of controls to future periods is subject to the risk that controls at a data processor may become inadequate or fail.

### **Opinion**

Our opinion has been formed on the basis of the matters outlined in this auditor's report. The criteria we used in forming our opinion are those described in the Data Processor's statement at pages 5 to 6. In our opinion, in all material respects:

- a. The description presents fairly GlobalConnect Outsourcing Services and the related technical and organisational measures and other controls, relating to processing and protection of personal data in accordance with the EU General Data Protection Regulation and the Danish Data Protection Act, as designed and implemented, throughout the period from 1 January to 31 December 2019.
- b. The technical and organisational measures and other controls, relating to the control objectives stated in the description were appropriately designed throughout the period from 1 January to 31 December 2019, and
- c. The technical and organisational measures and other controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the Description were achieved, operated effectively throughout the period from 1 January to 31 December 2019.

### **Description of Test of Controls**


The specific controls tested and the results of those tests are listed on pages 22 to 56.

### Intended Users and Purpose

This report is intended solely for data controllers who have used the Data Processor GlobalConnect Outsourcing Services, and who have a sufficient understanding to consider it along with other information, including information about the technical and organisational measures and other controls operated by the data controllers themselves in assessing whether the requirements of the EU General Data Protection Regulation and the Danish Data Protection Act have been complied with.

Copenhagen, 4 February 2020

### BDO Statsautoriseret revisionsaktieselskab



Claus Bonde Hansen  
State Authorised Public Accountant



Mikkel Jon Larssen  
Partner, Head of Risk Assurance, CISA



## GLOBALCONNECT A/S' STATEMENT

GlobalConnect A/S processes personal data in relation to GlobalConnect Outsourcing Services to our Customers, who are Data Controllers according to the Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the EU General Data Protection Regulation) and the Danish Act on Supplementary Provisions (the Danish Data Protection Act).

The description has been prepared for Data Controllers who have used GlobalConnect Outsourcing Services, and who have a sufficient understanding to consider the description along with other information, including information about the technical and organisational measures and other controls operated by the data controllers themselves in assessing whether the requirements of the EU General Data Protection Regulation and the Danish Data Protection Act have been complied with.

The Data Center department at GlobalConnect A/S is service sub-organisation in relation to the physical security in the data centers from which GlobalConnect Outsourcing Services are operated. The description does not include control objectives and controls managed by the Data Center department and thus includes solely control objectives and controls relating to processes and procedures managed by GlobalConnect Outsourcing Services (partial method).

GlobalConnect A/S uses a sub-processor. This sub-processor's relevant control objectives and related technical and organisational measures and other controls are not included in the accompanying description.

GlobalConnect A/S confirms that the accompanying description fairly presents GlobalConnect Outsourcing Services and the related technical and organisational measures and other controls throughout the period from 1 January to 31 December 2019. The criteria used in making this statement were that the accompanying description:

1. Presents how GlobalConnect Outsourcing Services, and how the related technical and organisational measures and other controls were designed and implemented, including:
  - The types of services provided, including the type of personal data processed;
  - The procedures used to ensure that data processing has taken place in accordance with contract, instructions or agreement with the data controller;
  - The procedures ensuring that the persons authorised to process personal data have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality;
  - The procedures ensuring upon discontinuation of data processing that, by choice of the data controller, all personal data are deleted or returned to the data controller unless retention of such personal data is required by law or regulation;
  - The procedures supporting in the event of breach of personal data security that the data controller may report this to the supervisory authority and inform the data subjects;
  - The procedures ensuring appropriate technical and organisational safeguards in the processing of personal data in consideration of the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed;
  - The controls that we, in reference to the scope of GlobalConnect Outsourcing Services, have assumed would be designed and implemented by the data controllers and which, if necessary in order to achieve the control objectives stated in the description, are identified in the description;

- The other aspects of the control environment, risk assessment process, information systems and communication, control activities and monitoring controls that are relevant to the processing of personal data;
2. Includes relevant information on changes in GlobalConnect Outsourcing Services and the related technical and organisational measures and other controls throughout the period from 1 January to 31 December 2019.
  3. Does not omit or distort information relevant to the scope of GlobalConnect Outsourcing Services and the related technical and organisational measures and other controls described while acknowledging that this description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of GlobalConnect Outsourcing Services that the individual data controllers might consider important in their particular circumstances.

GlobalConnect A/S confirms that the technical and organisational measures and other controls related to the control objectives stated in the description were appropriately designed and operated effectively throughout the period from 1 January to 31 December 2019. The criteria used in making this statement were that the accompanying description:

1. The risks that threatened achievement of the control objectives stated in the description were identified;
2. The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved; and
3. The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 1 January to 31 December 2019.

GlobalConnect A/S confirms that appropriate technical and organisational measures and other controls were implemented and maintained to comply with the agreements with data controllers, sound data processing practices and relevant requirements for data processors in accordance with the EU General Data Protection Regulation and the Danish Data Protection Act.

Taastrup, 31 January 2020

**GlobalConnect A/S**



Carsten Bryder  
Operations Director, COO



## **GLOBALCONNECT A/S' DESCRIPTION OF GLOBALCONNECT OUTSOURCING SERVICES**

### **GENERAL DESCRIPTION OF GLOBALCONNECT**

GlobalConnect A/S (GlobalConnect) is provider of Dark Fiber solutions, Transmission solutions, Outsourcing Services, including Cloud services, and Data Center solutions in Denmark, Northern Germany and parts of Sweden to a number of national and international telecom companies providing services to private and public businesses, universities and educational institutions. Services are also provided to Danish businesses.

GlobalConnect's vision is to be the leading telecom and data communications service provider in Denmark and Northern Germany and a key player in the markets where we are operating.

This description is prepared for the purpose of reporting on the IT general controls that GlobalConnect Outsourcing Services (GC-OS) applies to support and safeguard provision of IT operations to its customers. The description focuses on business-related control objectives and processes implemented to safeguard GC-OS' provision of IT operations.

The Data Center department at GlobalConnect is service sub-organisation in relation to the physical security in the data centers from which GC-OS is operated. This description does not include control objectives and controls managed by the Data Center department.

### **DESCRIPTION OF GLOBALCONNECT OUTSOURCING SERVICES' AND PROCESSING OF PERSONAL DATA**

GC-OS has since 2001 specialised in providing IT outsourcing and IT operation to a wide range of public and private businesses in the Danish market. As a medium-sized provider, GC-OS has been able to maintain a unique focus on supporting our customers' ability to operate an effective business in a public or private context. And what is more, this is without negative effects on the very fundamental IT capacities: stability, cost efficiency, scalability and, not least, operating reliability.

GC-OS has grown steadily over the years. The reason is not just intake of new customers but in particular also retention and extension of existing customer relations. Thus, we have throughout the years had a unique focus on customer satisfaction by means of quality assurance.

GC-OS has implemented a quality management system based on the requirements in ISO 9001:2015, which aims at continuously enhancement of the quality of all deliveries. This means that all parts of the delivery chain are subject to quality assurance; from appointment of suppliers, over internal policies for i.a. staff, compliance with all relevant public authority and regulatory requirements, to the quite central ITIL-founded operating processes. This means also that all potential improvements are identified currently; both those that we identify and those that our customers might identify.

Quite informally, outsourcing is about enhancing efficiency, and to utilise operation advantages, where possible. For IT operation purposes it is about creating maximum security for continuous and reliable operation of the entire IT portfolio. As a specialised sourcing-partner our principal duty is of course not only to provide 24/7 operations and maintenance, but also to ensure that this is done according to best practice within the area. In practice, this means that we deliver at the agreed service levels (SLAs and KPIs), and that the business relationship with us contributes actively to value creation and technological development for our customers. And our customers will have access to "critical mass" in the form of our core competences, namely technological operations, expert knowledge, processes and security. Our customers may thus release resources and focus on their core business.

For a number of the customers, GC-OS performs Managed Service (administration of IT platforms, including maintenance of Operating Systems and in some case support or integration systems (middleware). For





a larger number of customers, GC-OS offers Infrastructure as a Service (IaaS), where the customers themselves manage their IT setup and where GC-OS only provides HyperVisor platforms where GC-OS are not in contact with customer data.

GC-OS processes personal data on behalf of its customers, who are data controllers, when using services such as BaaS (Backup as a Service) or managing customer systems. GC-OS has made data processing agreements with the data controllers for this processing.

The personal data processed belong under article 6 of the Regulation on personal data and includes, for example, name, e-mail, telephone number and identification.

## GENERAL DESCRIPTION OF GLOBALCONNECT OUTSOURCING SERVICES' ORGANISATION

GC-OS is a Microsoft Silver Partner specialised in back-end products. GC-OS' staff are ITIL-certified, and senior project staff are PRINCE2-certified. Moreover, operations and project staff are currently certified within the technologies that are provided to our customers. The following organisational chart shows GC-OS' formal organisation of functions.



## MANAGEMENT OF PERSONAL DATA SECURITY

GC-OS is certified according to the international standard ISO 27001 and has implemented an Information Security Management System (ISMS) in accordance with the requirements of the standard.

GC-OS has set up requirements for establishment, implementation, maintenance and current improvement of an ISMS, so that this is managing the processing personal data. This is supported by agreements with the data controllers in which relevant requirements for data processors according to the General Data Protection Regulation and the Danish Data Protection Act are described.



The technical and organisational measures and other controls for protection of personal data are designed according to risk assessments and are implemented to ensure confidentiality, integrity and accessibility as well as compliance with applicable data protection legislation. Security measures and controls are as far as possible automated and technically supported by IT systems.

The management of the personal data security and technical and organisational measures and other controls are organised in the following main areas for which control objectives and control activities have been defined:

ISO 27001	Control activities	GDPR article
Risk assessment	<ul style="list-style-type: none"> <li>Risk assessment</li> </ul>	<ul style="list-style-type: none"> <li>Art. 28(3)(c)</li> </ul>
A.5: Information security policies	<ul style="list-style-type: none"> <li>Information Security Policy</li> <li>Personal Data Policy</li> <li>Review of policies</li> </ul>	<ul style="list-style-type: none"> <li>Art. 28(1)</li> </ul>
A.6: Organisation of information security	<ul style="list-style-type: none"> <li>Roles and responsibilities</li> <li>Remote workplaces and mobile equipment</li> <li>Authentications of external connections</li> </ul>	<ul style="list-style-type: none"> <li>Art. 28(1)</li> <li>Art. 28(3)(c)</li> </ul>
A.7: Human resource security	<ul style="list-style-type: none"> <li>Before employment</li> <li>During employment</li> <li>GDPR awareness</li> <li>Non-disclosure and confidentiality agreements</li> <li>End or change of employment</li> </ul>	<ul style="list-style-type: none"> <li>Art. 28(1)</li> <li>Art. 28(3)(b)</li> </ul>
A.8: Asset management	<ul style="list-style-type: none"> <li>Record of assets</li> <li>Record of categories of processing activities</li> <li>Ownership of assets</li> <li>Classification of assets</li> <li>Classification of information</li> </ul>	<ul style="list-style-type: none"> <li>Art. 30(2), (3) &amp; (4)</li> </ul>
A.9: Access management	<ul style="list-style-type: none"> <li>Policy for access management</li> <li>Access to network services</li> <li>User registration and deregistration</li> <li>Management of access rights</li> <li>Management of privileged access rights</li> <li>Management of password requirements</li> </ul>	<ul style="list-style-type: none"> <li>Art. 28(3)(c)</li> </ul>
A.10: Cryptography	<ul style="list-style-type: none"> <li>Administration of keys</li> </ul>	<ul style="list-style-type: none"> <li>Art. 28(3)(c)</li> </ul>
A.11: Physical and environmental security	<ul style="list-style-type: none"> <li>Physical perimeter safety guarding</li> <li>Physical access control</li> </ul>	<ul style="list-style-type: none"> <li>Art. 28(3)(c)</li> </ul>
A.12: Operations security	<ul style="list-style-type: none"> <li>Operations security procedures</li> <li>Change management</li> <li>Capacity management</li> <li>Separation of development, test and operation environments</li> <li>Backup</li> <li>Incident logging</li> <li>Administrator and operator logs</li> <li>Time synchronisation</li> </ul>	<ul style="list-style-type: none"> <li>Art. 28(3)(c)</li> </ul>
A.13: Communication security	<ul style="list-style-type: none"> <li>Policies and procedures for transfer of information</li> </ul>	<ul style="list-style-type: none"> <li>Art. 28(3)(c)</li> </ul>
A.14: Acquisition, development and maintenance of systems	<ul style="list-style-type: none"> <li>System acquisition, development and maintenance of systems</li> </ul>	<ul style="list-style-type: none"> <li>Art. 25</li> </ul>
A.15: Supplier relationships	<ul style="list-style-type: none"> <li>Agreements with sub-processors</li> <li>Approved sub-processors</li> <li>Supervision of sub-processors</li> </ul>	<ul style="list-style-type: none"> <li>Art. 28(2) &amp; (4)</li> </ul>
A.16: Information security incident management	<ul style="list-style-type: none"> <li>Handling of information and personal data security incidents</li> <li>Reporting of information and personal data security incidents</li> </ul>	<ul style="list-style-type: none"> <li>Art. 33(2)</li> </ul>



ISO 27001	Control activities	GDPR article
A.17: Information security aspects of disaster recovery, contingency and restore management	<ul style="list-style-type: none"> <li>Disaster recovery</li> <li>Security continuity</li> <li>Restore management</li> </ul>	<ul style="list-style-type: none"> <li>Art. 28(3)(c)</li> </ul>
A.18: Compliance	<ul style="list-style-type: none"> <li>Identification of applicable legislation</li> <li>Data protection agreements with customers</li> <li>Instruction from customers</li> <li>Assistance to the customers</li> <li>Deletion and return of customers data</li> <li>Independent review of controls</li> </ul>	<ul style="list-style-type: none"> <li>Art. 28(3)(a), (c), (e)-(h)</li> <li>Art. 29</li> <li>Art. 32(4)</li> <li>Art. 28(10)</li> </ul>

## RISK MANAGEMENT OF GLOBALCONNECT OUTSOURCING SERVICES

An annual risk assessment is carried out and input for this assessment is obtained from all levels in the organisation and by regulatory and public authority requirements. The process is facilitated by a quality and security committee consisting of executive staff from relevant departments. The assessment is presented to the company's senior management for approval. A contingency plan is also prepared annually which reflects the existing threat scenario.

Moreover, it is only natural that risks are assessed and managed at tactical and operational level. In practice, risk assessments are an explicit element of several of our ITIL-based operating processes and we record potential security-related incidents caused by both external and internal conditions in our Servicedesk system for the purpose of a subsequent analysis.

Risk assessments are based on the implementation guidelines in the international standard ISO27002.

The likelihood and consequence of the threats are reassessed based on the information existing at the present time. This reflects, in combination, the threat level. When the threat level is low, the need for security measures is lower than when the threat level is high. When the threat level has been determined, it is assessed to which extent the security environment considers the relevant threat level and it can be deduced herefrom how high the current remaining risk is.

GC-OS has a formal process for management of risks which result in specific action plans. The action plans are allocated and addressed according to the adopted RACI model.

The day-to-day Management of GlobalConnect decides on the basis of the risk assessment whether an identified risk can be accepted, is to be reduced or whether insurance is required based on selected risks.

This report includes solely controls and control objectives for processes and controls that are managed by GC-OS and, thus, it does not include controls or control objectives that are managed by sub-organisations.

## CONTROL FRAMEWORK, CONTROL STRUCTURE AND CRITERIA FOR CONTROL IMPLEMENTATION

GC-OS' information security is defined on the basis of the objective to provide dedicated IT outsourcing and high-quality infrastructure solutions, including stability and security.

The determination of criteria and scope of control implementation at GC-OS is based on the ISO 27002:2013 framework for management of information security. The following control areas in ISO 27002 were assessed:

- A.5. Information security policy
- A.6. Organisation of information security
- A.7. Human resource security
- A.8. Asset management



- A.9. Access management
- A.10. Cryptography
- A.11. Physical and environmental security
- A.12. Operations security
- A.13. Communications security
- A.14. Acquisition, development and maintenance of systems
- A.15. Supplier relationships
- A.16. Information security incident management
- A.17. Information security aspects of contingency, disaster recovery and restore management
- A.18. Compliance

### **Implemented control environment**

The implemented controls are based on the services provided by GC-OS to customers and include control areas and control activities within operation and hosting. All of the above areas are described in detail in the following in separate paragraphs, and the described control objectives and controls for those areas in the paragraph on control objectives, controls, tests and result of tests are an integral part of the description.

#### **A.5 Information security policy**

GC-OS has drawn up a formal information security policy with accompanying instructions which have been incorporated in an information security manual, one of the instructions in the manual describes GlobalConnect's classification policy which provides instructions for the management of information and data in the daily work. It is provided in connection with employment and all employees are also required to ensure they are updated periodically in relation to information security policy and the related manuals. Policies are approved annually, and manuals are approved by a cross-organisational committee when material changes are made. Finally, our suppliers/business partners are made familiar with the information security policy when obtaining non-disclosure agreements. The information security policy is reassessed annually by the Management.

#### **A.6 Organisation of information security**

GC-OS has implemented controls to ensure a general management of the information security including a delegation of responsibilities and handling of material risks in accordance with the requirements of the company's Management.

#### Management's obligations in relation to information security

Management takes an active part in the IT security in the organisation. The formal responsibility, including approval of the information security policy, is also that of the CEO.

#### Coordination of the information security

Activities to safeguard the information security are considered in a cross-organisational quality and security committee (KSU) with participants from all relevant departments.

#### Placing of responsibility for information security

All areas of responsibility for the IT security are described in GC-OS's security policy which clearly describes where the responsibility is placed in relation to information security and the contingency planning.

#### Placing of responsibility for data protection

The business' CEO is always responsible for the data protection. Management has delegated this responsibility to the Chief Information Security Officer (CISO) of the business. CISO manages together with staff in Quality, Risk & Compliance the operational responsibility for complying with personal data protection, internally and in relation to customer data.

#### Mobile data processing and communication

GC-OS' staff manual sets out guidelines for use of mobile equipment outside the company. Only equipment, which complies with GC-OS's security policy relating to protection against malicious code, can access the network from the outside and exclusively via VPN.

All remote work can solely be performed via our authorised PCs. Access from home workplace is secured via encrypted VPN connection, which requires validation via Active Directory.

#### Authentication of users on external connections

All access to our network, including external users, is authorised by our formal Access Management procedure, described in our quality manual.

#### Non-approved user equipment

Guest equipment and non-approved equipment, for example mobile phones, can solely be connected to a separate guest network.

### **A.7 Human resource security**

GC-OS has implemented controls to ensure that employees are qualified and conscious of their tasks and responsibilities in relation to information security.

For the purpose of employment at GC-OS, applicants must provide an unblemished criminal record which is subject to annual follow-up. Operational staff with access to customer data are also subject to security clearance by FE to minimum "Confidential".

#### Management's responsibility

As regards employees, they commit themselves, at their employment, to comply with the company's policies, including the security policy.

#### Awareness of information security and data protection, education and training

As regards employees, they are informed of all material changes to applicable policies and relevant procedures. This is done partly at the monthly meetings in the Quality and Security Committee and partly at staff meetings.

The employees are currently informed of personal data protection, so that there is a constant awareness of how employees manage the work with personally identifiable data, their own as well as the customers' data.

#### Roles and responsibilities

The responsibilities of the employees follow their place in the organisation. The responsibilities of all staff in relation to IT security are described in the staff manual, and where an increased responsibility applies this is described in the security policy.

#### Non-disclosure agreements

Confidentiality is part of the employment contracts. For a few customers there are special non-disclosure and confidentiality agreements and other security provisions for the employees working with the customer. Moreover, an overview has been prepared of all laws, requirements and security circulars that GC-OS must comply with. The list is reviewed annually by the administrative manager and the necessary renewals are made, if relevant.

#### Obligations relating to departures

General employment conditions, including conditions in relation to end of employment, are described in the employee's employment contract and the relating solemn declaration. Moreover, there is a formal procedure for departure which must be followed by the immediate manager. The HR manager is the ultimate responsible in this respect.



#### Return of equipment

All employees are to return all received material when the employment contract ends. This is done through a workflow placed at the HR department.

#### Closing of access rights

GC-OS's formal HR procedures ensure that all rights and physical access are withdrawn when an employment ends. This is done through a workflow placed in the HR department. Accesses are reviewed quarterly as part of our quality management system.

#### Sanctions relating to breach of the information security

In addition to common employment law provisions, the staff manual specifies sanctions. The workplace is subject to GC-OS' security routines which must not be broken. If this happens, it is considered a breach of the employment contract.

### **A.8 Asset management**

GC-OS has implemented controls to ensure achievement and maintenance of suitable protection of the organisation's equipment.

#### Registration of equipment

Relevant equipment, which is utilised, is registered in GC-OS' CMDB in service desk system, in which all changes are also registered. Moreover, there is an updated list of all authorised, mobile units. Non-utilised equipment is stated on an asset list and updated.

#### Record of categories of processing activities as a data processor

A record has been prepared of all data processing agreements and processing of personally identifiable data, which is administered in GlobalConnect. The record is stored electronically and only persons with a functional need to have access have rights and access hereto. At managerial level access to the records may be given by request if the request is sent to the Quality, Risk & Compliance department.

#### Accepted use of equipment

The employees' use of IT equipment and data is subject to fixed guidelines, defined in GC-OS' information security manual.

#### Management of portable media

The rules for use portable media is contained in the classification system described in the quality manual.

#### Procedures for information management

All processing of data follows the guidelines set out in the classification system for GC-OS.

The guidelines for processing of personally identifiable data comply with the guidelines set out in the information security policy and the accompanying information security manual. The information security policy sets out the guidelines for sanctions in case policy and manuals are not complied with.

### **A.9 Access management**

GC-OS has implemented controls to ensure that access to systems and data are granted through a documented process in accordance with a relevant work-related need and is closed down when the relevant access is no longer necessary.

#### Procedure for access control

As a supplement to our security policy, GC-OS has a formal procedure for access management.

#### Guidelines for use of network services

All user rights, including access to network, drives and applications, are determined on the basis of their function.

#### User creation

GC-OS has procedures for creation and closing down of users which are placed in our service desk system in the form of workflows.

#### Extended rights

All rights are managed on the basis of the employees' roles and are checked regularly in our quality management system. Extension of standard rights follows our formal access management procedure.

#### Management of password

Granting of passwords is subject to a number of rules which are set out in our Active Directory.

#### Reassessment of user access rights

All accesses and rights are reviewed periodically by the quality manager and the department managers.

#### User identification and authentication

GC-OS has separate admin-profiles for all operational staff on the systems where this is technically possible. All password validation is made via the OKTA systems which manages validation of the individual logins.

### **A.10 Cryptography**

GC-OS has implemented controls to ensure correct and effective use of cryptography to protect confidentiality, authenticity and/or integrity of data.

#### Data traffic

Backup data, sent via dedicated lines to the sub-organisation, are secured by one or more encryption keys.

### **A.11 Physical and environment security**

GC-OS has implemented controls to ensure that IT equipment is properly protected against unauthorised physical access and environmental incidents.

#### Physical access control

GC-OS' premises have access control in the form of a required personal code and a systems key to ensure that only authorised staff have access. Only GC-OS' employees receive a key and a code. If suppliers, consultants or other external parties are to have access, this is only possible together with authorised personnel.

#### Safeguarding of offices, premises and facilities

GC-OS' premises have access control in the form of a required personal code and a systems key to ensure that only authorised staff have access.

#### Protection against physical external threats

We refer to separate ISAE 3402 report on the description of controls, their design and operating effectiveness relating to GlobalConnect's Data Center solution.

#### Public areas, loading and unloading areas

Public access is only possible in the reception area. All other access is possible only together with authorised staff. Other entrance doors require a personal code. The unloading area at the ground floor is also separated by both a separate door and a rolling security shutter.

### Storing of equipment and protection of equipment

The critical equipment is placed in the server room to which only technical staff and GlobalConnect's partners have access.

## **A.12 Operations security**

GC-OS has implemented controls to ensure that operation of servers and key systems is carried out in a structured and secure manner.

### Documented operating procedures

All operating procedures are included in GC-OS' quality management system and are therefore easily available to all staff through our quality portal. They are all founded in ITIL and integrated in our service desk system. The quality management system involves maintenance and minimum one annual review of all procedures.

### Safeguarding of systems documentation

GC-OS keeps the systems documentation centrally in our CMDB in service desk, which can solely be accessed by authorised staff.

### Control of procedures for changes

We have a formal procedure for change management, which is based in our service desk system.

### Management of capacity

Monitoring of capacity has been implemented in relation to internet, network, servers, disk space and log files. GC-OS receives reporting from N-able and other tools which are used in the planning of purchase of additional capacity. Data from monitoring are registered and evaluated currently.

### Backup of information

Backup is taken of all important data according to customer agreements made. Errors in backup are identified by the TSM and Veeam backup tool and registered in GC-OS' service desk. Restore test for the customer is performed only when a specific agreement exists between the customer and GC-OS.

### Control of malicious code

All registered servers in GC-OS' infrastructure are updated with approved antivirus software according to Best Practice within the area. When a new server is set up, workflows in GC-OS' service desk ensure that antivirus is installed. All workstations in GC-OS are updated according to Best Practice with antivirus software. New workstations are installed with a standard image, which contains antivirus.

### Audit log

User transactions, exceptions and security incidents are logged, and the log is stored according to the retention periods agreed with the customer. Logging made from GC-OS' infrastructure is stored for an indefinite period of time.

### Use of monitoring systems

GC-OS has implemented internal procedures to ensure that alarms are addressed in order to respond to relevant incidents and act accordingly. All relevant alarms are shown on a big screen within normal working hours and to the on-duty officer during on-duty periods. All alarms are reviewed daily by GC-OS' operations department and are reported to customers because cases are created on the basis hereof.

### Incident logging

All incidents are registered in GlobalConnect's IT Service Management System. Incidents concerning breach in relation to the processing of personal data are always marked, so that they can rapidly be identified and dealt with by GlobalConnect's CISO.



#### Logging of administrator and operator

System administrators' actions are logged automatically in our service desk system and in Active Directory audit plus.

#### Logging of errors

Monitoring has been set up for the purpose of future analysis of errors and incidents in our service desk.

### **A.13 Communications security**

GC-OS has implemented controls to ensure that operation of material infrastructure components is carried out in a structured and secure manner.

#### Network controls

GC-OS has written procedures for configuration of firewalls, routers and switches, which are solely carried out by the operations department.

#### Security services on the network

Access to GC-OS' systems for our customers goes either through public networks where access is via VPN, MPLS and firewall. Access and communication between our servers and the internet go through our centrally managed firewall, where logging has been set up. All incoming network traffic goes through our firewalls. Only approved network traffic is allowed through the firewall based on a customer request.

#### Policies and procedures for data exchange

All data exchanges are as a minimum encrypted, meaning that they go via VPN or SSL encryption.

#### Control of network connections

Customer networks are limited by the VLAN and Access rules in our Core router / firewall. It is solely approved GC-OS personnel that can access the different customers' VLANs via the admin network physically on GC-OS.

### **A.14 Acquisition, development and maintenance of systems**

GC-OS has implemented controls to ensure that servers and relevant infrastructure components are updated and maintained as necessary and that this is done in a structured process.

#### Change management

GC-OS has a formal Change Management procedure to ensure that systems are reassessed and tested in connection with major changes and follows the process in our service desk system in the form of formalised workflows. Security patches are made once a month in the service windows agreed with the customers. All other service packs are installed solely at request and follows the process in our service desk system in the form of formalised workflows.

#### Control of technical vulnerabilities

Scanning for updates to systems is done by means of Shavlik Netcheck (Ivanti). Hereafter, GC-OS' formal procedure for patching is followed.

### **A.15 Supplier relationships**

GC-OS uses FRONT-SAFE as sub-supplier of backup. The service provided by FRONT-SAFE includes:

- Backup
- Status update

GC-OS uses G4S as sub-supplier of physical security and monitoring. The service provided by Vagtselskab includes:

- Monitoring of the physical location
- On-call services in case of alarm

#### Management of security in agreements with third party

If the sub-suppliers are an integral part of our services, we inspect the controls implemented by the supplier by obtaining an ISAE 3402 auditor's report.

In addition, relevant providers and consultants are to sign a non-disclosure agreement and confirm that they are familiar with our security policy.

To the extent that GC-OS' sub-suppliers store or otherwise manage personal data on behalf of GC-OS' customers in the course of the sub-supplier's provision of services to GC-OS, the sub-supplier acts as data processor solely according to instructions from GC-OS and GC-OS' customer. Thus, GC-OS's sub-suppliers commit themselves to take the necessary technical and organisational security measures to ensure that personal data are not accidentally or illegally destroyed, lost or impaired, and that they are not disclosed to unauthorised parties, misused or otherwise processed in violation of data protection legislation.

#### **A.16 Information security incident management**

GC-OS has established controls and guidelines which ensure that incidents are dealt with in time and that there is a follow-up on the incidents.

All incidents, including security incidents, follow our formal Incident/Problem Management or Request Fulfilment procedure. These are included in our quality management system and bases in our service desk system.

GC-OS has implemented procedures for documentation of all breaches of the management of personal data. Problem Management, which includes identification of the "root cause" of the breach of applicable guidelines for management of personal data, preventive and corrective measures. All procedures are available to employees with a functional need.

Procedures have been implemented on the basis of the data processing agreements with our customers. This is done to ensure correct management of security incidents within the agreed frame. A template has also been implemented to be used for reporting of breach of the Regulation to the data controller which ensures that all necessary information is provided, for the purpose of the further consideration on the part of the data controller.

#### **A.17 Information security aspects of contingency, disaster recovery and restore management**

GC-OS has prepared a contingency plan which is updated as required.

##### Information security integrated in the contingency plan

GC-OS has a formal contingency plan in which information security is incorporated.

##### Development and implementation of contingency plans which include information security

We have developed contingency plans to maintain or restore operations and ensure access to data at the required level and within acceptable time after failure or outage of critical business processes.

##### Responsibilities and guidelines

Roles and responsibilities are defined in the contingency plan. The operations manager and the contingency managers are responsible for different areas.

##### Contingency plan

GC-OS assesses risks regularly, and the contingency plan is updated to the existing risk exposure at least once a year in connection with Management's review and approval of the security policy.

##### Testing, maintenance and reassessment of contingency plans

The contingency plan is tested annually to ensure that it is applicable, sufficient and effective.



## A.18 Compliance with customer requirements and regulatory and public authority requirements

GC-OS has implemented controls to ensure that all relevant customer requirements and regulatory and public authority requirements are complied with.

### Compliance

As part of the customers' initialisation in GC-OS, procedures have been implemented to ensure that all customer requirements have been identified and addressed. Thus, project management is used to manage the customers' implementation in GC-OS' operations environment.

GC-OS has prepared an overview containing all relevant regulatory and public authority requirements to be complied with in relation to the operations environment.

### Privacy and protection of personal data

GC-OS stores and processes personal data as instructed by the customer for the customers who have made data processing agreements with us.

### Signing of data processing agreements

GC-OS has implemented procedures for making data processing agreements which ensure that GC-OS in relation to the contract with the customers signs a data processing agreement which describes the terms for processing of personal data on behalf of the data controller. GC-OS uses a template for data processing agreements in accordance with the services delivered, including information on the use of sub-processors. The data processing agreements are signed digitally and stored electronically.

### Instruction for processing of personal data

GC-OS has implemented procedures which ensure that GC-OS acts according to the instruction given by the data controller in the data processing agreement. The instruction is maintained in the company's classification system which instructs the employees how the processing of personal data is to be made, including the persons at the data controller that can give binding instructions to GC-OS. The instruction ensures also that GC-OS informs the data controller when the controller's instruction is contrary to the data protection legislation.

### Assistance to the data controller

GC-OS has implemented instructions which ensure that GC-OS can assist the data controller in complying with his obligations to respond to requests for exercising of the data subjects' rights.

GC-OS has implemented instructions which ensure that GC-OS can assist the data controller in complying with the obligations in article 32 on security of processing, article 33 on reporting and notification of breach of the personal data security, and articles 34 to 36 on impact assessments.

GC-OS has implemented instructions which ensure that GC-OS can make available all information required to prove compliance with the requirements for data processors to the data controller. GC-OS also enables and contribute to audits, including inspections, made by the data controller or other parties authorised by the data controller.

### Deletion and return of customers data

GC-OS has implemented instructions which ensure that personal data are deleted or returned according to the data controller's instruction when the processing of personal data ends on expiry of the contract with the data controller. The customer's personal data remains in the company's classification system until the customer finally approves the frames for off-boarding, including deletion of data and the relevant circumstances.

### Independent review of controls

A large part of the procedures and the underlying controls is included in our ISO 9001 certified quality management system, which besides regular internal audits also is subject to an annual, external audit.

Finally, GC-OS is ISO27001 certified within information security. As a part of this, procedures have been prepared for annual reassessment and approval of underlying policies, description of processes and procedures, and this is audited annually.

Compliance with the EU General Data Protection Regulation is confirmed by annually obtaining an independent auditor's report which supports the company's compliance with the Regulation.

## **CHANGES TO SERVICES AND RELATING CONTROLS**

In the period from 1 January to 31 December 2019 no material changes were made to GlobalConnect's services within Outsourcing Services and relating controls.

## **SUPPLEMENTARY INFORMATION ON THE IMPLEMENTED CONTROL ENVIRONMENT**

### **Conditions to be observed by the customer**

To achieve the above specified control objectives, the following controls must be implemented and correctly managed by the user organisations:

#### User administration

GC-OS grants access to internal staff and manages the user administration. GC-OS carries out user administration of customers' staff if an agreement has been made for this purpose. The user administration is carried out at the request of the customer. It is the customer's responsibility to ensure that GC-OS receives the correct information in relation to the user administration.

#### Configuration of security

GC-OS has implemented security on the network layer in the form of segmentation, requirements for password and logging. If the security on the customer servers is not configured by GC-OS, it is the customers' responsibility to ensure security on servers hosted at GC-OS. When GC-OS installs servers, a baseline is used to ensure suitable security on the servers.

#### Disaster recovery

GC-OS has implemented controls to ensure that backup is taken of data, and that the readability of the back is checked regularly. If complete systems are to be restored, GC-OS ensures that backup copies of data are available for the restore of the system where GC-OS's customers are themselves responsible for restoring of the systems. If complete systems are to be restored and an agreement has been made for this purpose, GC-OS will ensure that this is possible and will test this according to the agreement.

#### Protection of equipment at GC-OS' customers

GC-OS has implemented controls for physical protection of equipment placed at GC-OS, including equipment placed at GC-OS' data center. Protection of the equipment includes, among others, restrictions on the physical access to the relevant equipment. GC-OS' customers are responsible for physical safeguarding of equipment placed in their own physical environment.

## CONTROL OBJECTIVES, CONTROL ACTIVITIES, TESTS AND RESULT OF TESTS

### Objective and scope

We conducted our engagement in accordance with ISAE 3000, Assurance Reports Other Than Audits or Reviews of Historical Financial Information.

BDO has performed procedures to obtain evidence of the information in GlobalConnect A/S' description of GlobalConnect Outsourcing Services and the design and operating effectiveness of the relating technical and organisational measures and other controls. The procedures elected depend on BDO's assessment, including the assessment of the risks that the description is not fairly presented and that the controls are not appropriately designed and operating effectively.

BDO's test of the design and the operating effectiveness of the relating technical and organisational measures and other controls and their implementation has included the control objectives and related control activities selected by GlobalConnect A/S, and which are described in the check form below.

In the test form, BDO has described the tests carried out which were assessed necessary to obtain reasonable assurance that the stated control objectives were achieved, and that the related controls were appropriately designed and operated effectively throughout the period from 1 January to 31 December 2019.

### Test procedures

Test of the design of the relating technical and organisational measures and other controls and their implementation was performed by inquiries, inspection, observation and re-performance.

Type	Description
Inquiry	Inquiries of relevant personnel have been performed for all significant control activities.  The purpose of the inquiries was to obtain knowledge and further information about implemented policies and procedures, including how the control activities are performed, and to obtain confirmed evidence of policies, procedures and controls.
Inspection	Documents and reports, which include information about the performance of the control, have been read for the purpose of assessing the design and monitoring of the specific controls, i.e. whether the design of the controls is such that they are expected to be effective if implemented, and whether the controls are sufficiently monitored and checked at suitable intervals.  Tests have been performed of significant system structures of technical platforms, databases and network equipment to ensure that controls have been implemented, including for example assessment of logging, back-up, patch management, authorisations and access controls, data transmission, and inspection of equipment and locations.
Observation	The use and existence of specific controls have been observed, including tests to ensure that the control has been implemented.
Re-performance	Controls have been re-performed to obtain additional evidence that the controls operate as assumed.

For the services provided by Frontsafe A/S within back-up of the operating systems, we have from an independent auditor received an ISAE 3402 report for the period from 1 October 2018 to 30 September 2019 on technical and organisational security measures relating to operation of Cloud Backup services.

This sub-processors' relevant control objectives and related controls are not included in GlobalConnect A/S' description of services and relevant controls related to operation of GlobalConnect Outsourcing Services. Accordingly, we have solely assessed the report and tested the controls at GlobalConnect that monitor the operating effectiveness of the sub-processor's controls and ensure proper supervision of the sub-processor's compliance with the data processing agreement made by the sub-processor and the data processor and compliance with the General Data Protection Regulation and the Danish Data Protection Act.

**Result of test**

The result of the test made of technical and organisational measures and other controls has resulted in the following exceptions noted.

An exception exists when:

- Technical and organisational measures and other controls have not been designed or implemented to fulfil a control objective,
- Technical and organisational measures and other controls related to a control objective are not suitably designed and implemented or did not operate effectively throughout the period.

Risk assessment		
Control Objective		
<p>► To ensure that the data processor carries out an annual risk assessment in relation to the consequences for the data subjects which forms basis for the technical and organisational measures.</p>		
Control Activity	Test performed by BDO	Result of test
<p><b>Risk assessment</b></p> <ul style="list-style-type: none"> <li>► A risk assessment is performed annually which is laid before and assessed by Management. The risk assessment is a part of the work with GlobalConnect's information security management system (ISMS).</li> <li>► An annual risk assessment is carried out that provides the basis for data protection reasoned implementations.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected the GlobalConnect's information security policy, information security rules, and information security manual. We observed that the overall risk assessment is part of the work with the information security management system.</p> <p>We have inspected the service GlobalConnect's risk assessment. We observed that the risk assessment applies to 2019. We were informed that threats and risks are assessed currently by the Quality and Security Committee.</p> <p>We observed that meetings are held regularly in the GlobalConnect's Quality and Security Committee, and we have inspected selected minutes of meetings. We observed that the purpose of the meetings is to ensure maintenance, raising and embedding of information security, including current assessment of threats and risks.</p> <p>We have inspected GlobalConnect's Personal Data Policy and risk assessment. We have observed that the risk assessment is part of the work with the information security management system.</p> <p>We have observed that the risk assessment is part of the work with data protection.</p>	<p>We have observed that the risk assessment does not include assessment of risks and consequences for the data subjects.</p> <p>No other deviations identified.</p>

A.5: Information security policies		
Control Objective		
<p>▶ To provide guidelines for and supporting information security and data protection in accordance with business requirements and relevant laws and regulations. GDPR art. 28, paragraph 1, art. 28, paragraph 3, point c.</p>		
Control Activity	Test performed by BDO	Result of test
<p><b>Policies for information security</b></p> <p>▶ Management sets out and approves policies for information security which after approval are published and communicated to staff and relevant external parties.</p>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's information security policy, information security rules, and information security manual. We observed that the information security policy has been designed in accordance with ISO 27001/27002.</p> <p>We have inspected GlobalConnect's terms of reference for the Quality and Security Committee set up, including procedures to ensure approval by management and communication within the organisation.</p> <p>We have inspected the information security policy.</p> <p>We observed that the information security policy is communicated to employees and relevant external business partners and we have inspected relevant documentation.</p>	<p>No deviations identified.</p>
<p><b>Policies for personal data protection</b></p> <p>▶ GlobalConnect has prepared a written information security manual, which includes managing of personal data.</p> <p>▶ GlobalConnect has prepared and implemented a Personal Data Policy.</p>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's information security manual and Personal Data Policy.</p> <p>We have observed that the information security manual and Personal Data Policy is communicated to employees and we have inspected relevant documentation.</p>	<p>No deviations identified.</p>
<p><b>Review of policies for information security</b></p> <p>▶ GlobalConnect has implemented an annual plan of controls which ensures periodical review of the information security policy.</p> <p>▶ A written information security policy has been drawn up which is reassessed annually.</p> <p>▶ The information security policy is updated and approved by Management.</p>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's audit plan for review of information security policy, information security rules, and information security manual.</p> <p>We observed that a written information security policy has been drawn up which describes that the policy is reassessed annually.</p>	<p>We found that the information security policy has not been approved by the Senior Management's signing in 2019.</p> <p>We found that GlobalConnect's Personal Data Policy and data classification policy has not been reviewed and updated in 2019.</p> <p>No other deviations identified.</p>



## A.5: Information security policies

### Control Objective

- ▶ *To provide guidelines for and supporting information security and data protection in accordance with business requirements and relevant laws and regulations. GDPR art. 28, paragraph 1, art. 28, paragraph 3, point c.*

Control Activity	Test performed by BDO	Result of test
<ul style="list-style-type: none"> <li>▶ The Personal Data Policy is reviewed and approved on an ongoing basis.</li> <li>▶ The information security manual is reviewed and approved by management on an ongoing basis, as a minimum once a year during the annual review.</li> </ul>	<p>We observed that the information security policy was updated in December 2019.</p> <p>We have inspected GlobalConnect's Personal Data Policy and information security manual.</p>	

A.6: Organisation of information security		
<b>Control Objective</b> ▶ To establish a management basis for initiating and managing the implementation and operation of information security and data protection in the organisation. GDPR art. 37, paragraph 1. ▶ To secure remote workplaces and the use of mobile equipment. GDPR art. 28, paragraph 3, point c.		
Control Activity	Test performed by BDO	Result of test
<b>Roles and responsibilities</b> <ul style="list-style-type: none"> <li>▶ The responsibility for the information security in GlobalConnect lies with the management.</li> <li>▶ Management has appointed a cross-organisational Quality and Security Committee which considers activities relating to safeguarding of the information security.</li> <li>▶ Management has designated a Quality and Security Manager who has the overall responsibility for handling the information security.</li> <li>▶ Responsibility for data protection in GlobalConnect is assigned by management to the Quality and Security Manager and his department for Quality, Risk &amp; Compliance.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's information security policy, information security rules, and information security manual and overview of the in-house organisation of the information security.</p> <p>We have inspected GlobalConnect's terms of reference for the Quality and Security Committee set up, procedure for the quality and security work, and the quality manual, including document handling.</p> <p>We observed that meetings are held regularly in GlobalConnect's Quality and Security Committee, and we have inspected selected minutes of meetings. We observed that the purpose of the meetings is to ensure maintenance, raising and embedding of information security.</p> <p>We have inspected GlobalConnect's data classification policy and documentation for awareness concerning the responsibility for data protection in GlobalConnect.</p> <p>We have observed that GlobalConnect has an overview of the department, Quality, Risk &amp; Compliance's responsibility, which is accessible for the employees and information about how employees can reach the department in case of data protection questions and breaches of data protection.</p> <p>We have observed that GlobalConnect's data classification policy should be reviewed and reassessed once a year as the procedure prescribe.</p>	<p>No deviations identified.</p>

A.6: Organisation of information security		
<b>Control Objective</b> ▶ To establish a management basis for initiating and managing the implementation and operation of information security and data protection in the organisation. GDPR art. 37, paragraph 1. ▶ To secure remote workplaces and the use of mobile equipment. GDPR art. 28, paragraph 3, point c.		
Control Activity	Test performed by BDO	Result of test
<b>Remote workplaces and mobile equipment</b> ▶ Updated antivirus must be installed on all mobile units used for work-related purposes. ▶ Connection to internal units must go via two-factor authentication (SMS Passcode or Direct Access).	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's information security manual and information security rules.</p> <p>We have inspected GlobalConnect's use of antivirus programme on mobile units, including that the antivirus system is updated regularly. We inspected extracts which show the status of installation and updating of antivirus on all units.</p> <p>We have inspected GlobalConnect's information security rules relating to remote workplaces and mobile equipment.</p> <p>We have observed that GlobalConnect uses End-point Security to VPN, and that End-point Security is set up with two-factor approval on mobile equipment in relation to remote workplaces.</p>	<p>We found that there are 5 units for which the status for anti-malware is "off".</p> <p>No other deviations identified.</p>
<b>Authentication of external connections</b> ▶ All external units connecting to GlobalConnect's internal network must be covered by two-factor solutions.	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's information security manual and information security rules.</p> <p>We have inspected GlobalConnect's information security rules relating to remote workplaces and mobile equipment.</p> <p>We have observed that GlobalConnect's uses End-point Security to VPN, and that End-point Security is set up with two-factor approval on mobile equipment in relation to remote workplaces, and that external units are covered by the same two-factor solution.</p> <p>We have observed that external visitors have access only to GlobalConnect's guest network which is password protected.</p>	<p>No deviations identified.</p>

A.7: Human resource security		
<p><b>Control Objective</b></p> <ul style="list-style-type: none"> <li>▶ To ensure that employees and contracting parties understand their responsibilities and are suitable for the roles they are intended. GDPR art. 28, paragraph 1, art. 28, paragraph 3, art. 37, paragraph 1.</li> <li>▶ To ensure that employees and contracting parties are aware of and meet their information security responsibilities. GDPR art. 28, paragraph 1, art. 28, paragraph 3, point c.</li> <li>▶ To protect the organization's interests as part of the change or termination of the employment relationship. GDPR art. 28, paragraph 3, point b.</li> </ul>		
Control Activity	Test performed by BDO	Result of test
<p><b>Before employment</b></p> <ul style="list-style-type: none"> <li>▶ A background check is made of all job candidates in accordance with business requirements and the function to be held by the employee.</li> <li>▶ Employment at GlobalConnect requires always that an unblemished criminal record can be shown.</li> <li>▶ When the customer or the task requires security clearance, this is obtained for the relevant employees in accordance with the relevant procedure for this purpose.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's procedure for employment and departure of staff. We observed that a background check is made as part of the employment process, and we have inspected the approved employment contract template.</p> <p>We have inspected the form to be used for new employees which among others contain information on the areas to which the individual employees are to have access to the programmes and rights the employee should be granted. We observed that the form is issued by HR and approved by the immediate manager.</p> <p>We have inspected an overview of new employees in 2019, and we have by random sampling selected and inspected documentation for new employees which follows GlobalConnect's procedures in this respect, including creation of employees in systems and presentation of criminal record.</p> <p>We have inspected a list of the employees who have obtained security clearance from the Danish Defence Intelligence Service.</p>	<p>No deviations identified.</p>
<p><b>During employment</b></p> <ul style="list-style-type: none"> <li>▶ Employees at GlobalConnect are currently informed of information security matters and potential threats in relation to their tasks.</li> <li>▶ Employees at GlobalConnect declare annually that they have read and accept the information security policy and the manual.</li> <li>▶ Awareness campaigns towards GlobalConnect employees are performed several times a year to ensure continuous focus on data protection and security.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's Intranet. We have observed that the employees at GlobalConnect are kept updated on information security matters and any threats relating to their tasks.</p>	<p>No deviations identified.</p>

## A.7: Human resource security

### Control Objective

- ▶ To ensure that employees and contracting parties understand their responsibilities and are suitable for the roles they are intended. GDPR art. 28, paragraph 1, art. 28, paragraph 3, art. 37, paragraph 1.
- ▶ To ensure that employees and contracting parties are aware of and meet their information security responsibilities. GDPR art. 28, paragraph 1, art. 28, paragraph 3, point c.
- ▶ To protect the organization's interests as part of the change or termination of the employment relationship. GDPR art. 28, paragraph 3, point b.

Control Activity	Test performed by BDO	Result of test
	<p>We have inspected publications to the employees on selected subjects within information security and data protection legislation. We have observed that the publications have been included in information campaigns, etc.</p> <p>We inspected a list of personnel starting in 2019 and we have randomly selected and inspected documentation for new employees which complies with GlobalConnect's procedures in this respect, including confirmation by their signature that they have read and accepted the information security policy and manual.</p> <p>We have inspected GlobalConnect's awareness communication plan and performed awareness activities in 2019. We have observed that GlobalConnect has performed awareness activities towards the employees during the year according to the awareness communication plan.</p> <p>We have observed that GlobalConnect employees have access to an overview of different data protection awareness materials and use different channels to inform the employees about data protection guidelines in GlobalConnect.</p>	
<p><b>Non-disclosure and confidentiality agreements</b></p> <ul style="list-style-type: none"> <li>▶ All employees working with confidential data - including personal data - have signed a non-disclosure agreement.</li> <li>▶ The employees are bound by a confidentiality agreement both internally and towards the customers.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's process for employment of new staff and approved employment contract template. We observed that the employment contract includes conditions on confidentiality, applicable during employment and at the end of employment and for both in-house and customer-related data.</p>	No deviations identified.

A.7: Human resource security		
<b>Control Objective</b> <ul style="list-style-type: none"> <li>▶ To ensure that employees and contracting parties understand their responsibilities and are suitable for the roles they are intended. GDPR art. 28, paragraph 1, art. 28, paragraph 3, art. 37, paragraph 1.</li> <li>▶ To ensure that employees and contracting parties are aware of and meet their information security responsibilities. GDPR art. 28, paragraph 1, art. 28, paragraph 3, point c.</li> <li>▶ To protect the organization's interests as part of the change or termination of the employment relationship. GDPR art. 28, paragraph 3, point b.</li> </ul>		
Control Activity	Test performed by BDO	Result of test
	<p>We have inspected randomly selected employment contracts and observed that the conditions for confidentiality are described and that the employment contract is signed by the employee.</p> <p>We have inspected GlobalConnect's process for employment of new staff and approved employment contract template. We observed that the employment contract includes conditions on confidentiality, applicable during employment and at the end of employment and for both in-house and customer-related data.</p> <p>We have inspected randomly selected employment contracts and observed that the conditions for confidentiality are described and that the employment contracts are signed by the employees.</p>	
<b>End or change of employment</b> <ul style="list-style-type: none"> <li>▶ After the end or change of the employment, accesses and rights are withdrawn or changed in accordance with the functional need in this respect.</li> <li>▶ After the end of the employment, equipment received by the leaving employee is returned.</li> <li>▶ After the end of the employment, HR ensures that the procedure for departure is complied with.</li> <li>▶ GlobalConnect has defined rules in their employment contracts concerning off-boarding.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's procedure for employment and departure of employees. We have inspected the form used in connection with departure.</p> <p>We observed that OMC/IT and the employee sign the departure form for closing of access cards and return of GlobalConnect's physical equipment. The departure form is kept in the HR manager's physical files.</p> <p>We have inspected overview of employees who left in 2019, and we inspected resignation form for randomly selected employees, who have left.</p>	No deviations identified.

## A.7: Human resource security

### Control Objective

- ▶ *To ensure that employees and contracting parties understand their responsibilities and are suitable for the roles they are intended. GDPR art. 28, paragraph 1, art. 28, paragraph 3, art. 37, paragraph 1.*
- ▶ *To ensure that employees and contracting parties are aware of and meet their information security responsibilities. GDPR art. 28, paragraph 1, art. 28, paragraph 3, point c.*
- ▶ *To protect the organization's interests as part of the change or termination of the employment relationship. GDPR art. 28, paragraph 3, point b.*

Control Activity	Test performed by BDO	Result of test
	<p>We have inspected GlobalConnect's employment contract template and observed that the employment contract includes confidentiality, applicable after termination of employment for both in-house and customer-related data.</p> <p>We have inspected randomly selected employment contracts and observed that the conditions for confidentiality are contained in the employment contracts and are signed by the employees.</p>	

## A.8: Asset management

### Control Objective

- ▶ To identify the organization's assets and define appropriate responsibilities for its protection. GDPR art. 30, paragraph 2, art. 30, paragraph 3, art. 32, paragraph 2.
- ▶ To ensure adequate protection of information and personal data that is in relation to the importance of the information and personal data for the organization. GDPR art. 30, paragraph 3, art. 30, paragraph 4.
- ▶ To prevent unauthorized disclosure, modification, removal or destruction of information and personal data stored on media. GDPR art. 28, paragraph 3, point c.

Control Activity	Test performed by BDO	Result of test
<b>Record of assets</b> <ul style="list-style-type: none"> <li>▶ All equipment relevant to provision of services is identified and recorded in CMDB, in which changes are also recorded.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's information security rules.</p> <p>We have inspected the CMDB system and observed that changes relating to equipment are recorded, and the owner of the different assets is recorded.</p> <p>We have inspected list of customers in GlobalConnect for 2019, and we have by random sampling selected and inspected documentation that the customers' assets are identified and registered in CMDB.</p> <p>We inspected GlobalConnect's list of hardware.</p>	No deviations identified.
<b>Record of categories of processing activities</b> <ul style="list-style-type: none"> <li>▶ GlobalConnect has prepared a record of processing activities, which is kept updated occasionally - at least once a year.</li> <li>▶ The record is kept electronically.</li> <li>▶ GlobalConnect makes the record available to the supervisory authority on request.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's record of processing activities as processor. We observed that GlobalConnect has prepared a record of categories of processing activities on behalf of the customers.</p> <p>We have furthermore observed that the record is kept electronically and includes the elements required according to General Data Protection Regulation article 30(2).</p> <p>We have observed that the record is updated regularly and on inquiry, we were informed that the record is made available to the supervisory authority on request.</p> <p>We were not able to verify that GlobalConnect makes the record available to the supervisory authority on request, because no requests have been made for this purpose.</p>	No deviations identified.



## A.8: Asset management

### Control Objective

- ▶ To identify the organization's assets and define appropriate responsibilities for its protection. GDPR art. 30, paragraph 2, art. 30, paragraph 3, art. 32, paragraph 2.
- ▶ To ensure adequate protection of information and personal data that is in relation to the importance of the information and personal data for the organization. GDPR art. 30, paragraph 3, art. 30, paragraph 4.
- ▶ To prevent unauthorized disclosure, modification, removal or destruction of information and personal data stored on media. GDPR art. 28, paragraph 3, point c.

Control Activity	Test performed by BDO	Result of test
<b>Ownership of assets</b> <ul style="list-style-type: none"> <li>▶ An owner has been designated for all IT equipment at all customers.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's information security rules.</p> <p>We inspected the CMDB systems and randomly observed that the ownership has been established for all assets for all customers.</p>	No deviations identified.
<b>Classification of assets</b> <ul style="list-style-type: none"> <li>▶ Guidelines are prepared for classification of information and data. All processing of media and data are performed according to GlobalConnect's classification system.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's data classification policy and observed the guidelines for managing portable media and processing of information and data.</p> <p>On inquiry we were informed that all media and data are in practice classified as confidential and treated in accordance with GlobalConnect's procedures in this respect.</p>	No deviations identified.
<b>Classification of information</b> <ul style="list-style-type: none"> <li>▶ The different information handled and managed by the organisation has been identified and separated into categories reflecting the consequences if the information was compromised.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's data classification policy and observed that GlobalConnect has guidelines for processing and securing of different information, including personal data.</p> <p>We observed that the guidelines for processing of personal data are accessible for employees.</p>	No deviations identified.

A.9: Access management		
<b>Control Objective</b> <ul style="list-style-type: none"> <li>▶ To restrict access to information and personal data, including information and personal data processing facilities. GDPR art. 28, paragraph 3, point c.</li> <li>▶ To ensure access for authorized users and prevent unauthorized access to systems and services. GDPR art. 28, paragraph 3, point c.</li> <li>▶ To make users responsible for securing their authentication information. GDPR art. 28, paragraph 3, point c.</li> <li>▶ To prevent unauthorized access to systems and applications. GDPR art. 28, paragraph 3, point c.</li> </ul>		
Control Activity	Test performed by BDO	Result of test
<b>Policy for access management</b> <ul style="list-style-type: none"> <li>▶ Processes and procedures have been adopted to manage access and restrictions to systems and data based on business and functional requirements.</li> <li>▶ All access and changes to access to systems and data follow the adopted processes and procedures.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's procedure for employment and departure of employees, procedure for access control to physical locations and systems and procedure for escorted access to GlobalConnect's data centres and other locations.</p> <p>Based on inspection of documentation for the following areas under A.9, we observed that the adopted processes and procedures are complied with.</p>	No deviations identified.
<b>Access to network services</b> <ul style="list-style-type: none"> <li>▶ GlobalConnect grants access to network and network services according to the "need-to-know" principles (access according to function).</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected extract from Active Directory and observed that the users are granted different rights to different services, managed via Group Policy in Active Directory.</p>	No deviations identified.
<b>User registration and deregistration</b> <ul style="list-style-type: none"> <li>▶ GlobalConnect has implemented and follows the process for creation and deregistration of users in systems.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's procedure for employment and departure of employees. We have inspected the form to be completed for new employees and the form relating to departure.</p> <p>We have inspected overview of new employees and employees who left in 2019, and we have randomly selected and inspected documentation for new employees and employees, who have left, which follows GlobalConnect's procedures in this respect. We observed that GlobalConnect performs its own controls by which the users' access is checked.</p>	No deviations identified.

A.9: Access management		
<b>Control Objective</b> <ul style="list-style-type: none"> <li>▶ To restrict access to information and personal data, including information and personal data processing facilities. GDPR art. 28, paragraph 3, point c.</li> <li>▶ To ensure access for authorized users and prevent unauthorized access to systems and services. GDPR art. 28, paragraph 3, point c.</li> <li>▶ To make users responsible for securing their authentication information. GDPR art. 28, paragraph 3, point c.</li> <li>▶ To prevent unauthorized access to systems and applications. GDPR art. 28, paragraph 3, point c.</li> </ul>		
Control Activity	Test performed by BDO	Result of test
<b>Granting, adjustment and withdrawal of access rights</b> <ul style="list-style-type: none"> <li>▶ GlobalConnect has implemented a procedure for granting of user access for the purpose of granting access rights for all types of users to all systems and services.</li> <li>▶ GlobalConnect has implemented a process for withdrawal or adjustment of access rights, including deletion of an employee's access when moving or leaving.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's procedure for employment and departure of employees.</p> <p>We have inspected the form to be completed for employees which among others contain information on the areas to which the individual employee should have access and the programmes and rights that should be granted to the employee. We observed that the form is issued by HR and approved by the immediate manager.</p> <p>We have inspected the departure form used.</p> <p>We inspected list of employees starting in 2019 and we have randomly selected and inspected documentation for new employees. We observed that GlobalConnect's procedures in this respect are complied with, including granting of access to systems and services.</p> <p>We have randomly selected employees from a list of all employees resigned in 2019 and examined whether their access to the network was timely disabled.</p>	<p>We found that two resigned employees continue to have access to Active Directory.</p> <p>No other deviations identified.</p>
<b>Management of privileged access rights</b> <ul style="list-style-type: none"> <li>▶ GlobalConnect has implemented granting of administrative access to entities according to the functional need which is authorised.</li> <li>▶ GlobalConnect has implemented logging of accesses with privileged accounts (administrative rights).</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's procedure for employment and departure of employees.</p> <p>We have inspected the form to be completed for employees which among others contain information on the areas to which the individual employee should have access and the pro-</p>	<p>We found that there is no documentation that 24 Enterprise Admins, 60 Domain Admins and 94 Built-in Admins have these rights based on functional needs.</p> <p>No other deviations identified.</p>

A.9: Access management		
<b>Control Objective</b> <ul style="list-style-type: none"> <li>▶ To restrict access to information and personal data, including information and personal data processing facilities. GDPR art. 28, paragraph 3, point c.</li> <li>▶ To ensure access for authorized users and prevent unauthorized access to systems and services. GDPR art. 28, paragraph 3, point c.</li> <li>▶ To make users responsible for securing their authentication information. GDPR art. 28, paragraph 3, point c.</li> <li>▶ To prevent unauthorized access to systems and applications. GDPR art. 28, paragraph 3, point c.</li> </ul>		
Control Activity	Test performed by BDO	Result of test
	<p>grammes and rights that should be granted to the employee, including granting of administrative access. We observed that the form is issued by HR and approved by the immediate manager.</p> <p>We have inspected overview of new employees in 2019, and we have randomly selected and inspected documentation for new employees, which follows GlobalConnect's procedures in this respect, including granting of access to systems and services.</p> <p>We inspected extracts of users with privileged rights.</p> <p>We have observed that GlobalConnect has implemented a system for management, monitoring and logging of privileged accounts.</p> <p>We have inspected the audit policy in GlobalConnect's network operating system, which ensures logging of access by users with privileged/administrative rights.</p>	
<b>Management and use of passwords to users</b> <ul style="list-style-type: none"> <li>▶ GlobalConnect has implemented a process and rules for granting and management of passwords.</li> <li>▶ GlobalConnect has implemented rules for establishment of passwords which must be followed by all employees.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's information security rules and information security manual for use of passwords, including procedure for user access to IT systems.</p> <p>We have inspected the password policy and the audit policy in GlobalConnect's network operating system. We have observed that management of passwords has been set up.</p>	No deviations identified.

## A.10: Cryptography

### Control Objective

- ▶ To ensure the correct and effective use of cryptography to protect the confidentiality, authenticity and / or integrity of information and personal data. GDPR art. 28, paragraph 3, point c.

Control Activity	Test performed by BDO	Result of test
<b>Administration of keys</b> <ul style="list-style-type: none"> <li>▶ Processes and procedures are implemented for creation and maintenance of encryption keys at the customers who have specified the need in their contract with GlobalConnect.</li> <li>▶ Backup data are transmitted over dedicated lines to the sub-organisation and safeguarded by one or more encryption keys.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected procedures for creation or renewal of encryption keys.</p> <p>We have inspected the procedure of certificate check of N'able.</p> <p>We have inspected the overview in Service Management System of all customers who have purchased a certificate and we have observed that the certificates are updated.</p> <p>We observed that data are encrypted with 128-bit AES to safeguard the confidentiality, authenticity and integrity of information.</p> <p>We have received and inspected agreements made, including Service Level Agreement, with Frontsafe A/S on Cloud Backup services and ISAE 3402 type 2 report for the period from 1 October 2018 to 30 September 2019.</p>	<p>No deviations identified.</p>

## A.11: Physical and environmental security

### Control Objective

- ▶ To prevent unauthorized physical access to, and damage/disruption of the organization's information and personal data, including information- and personal data processing facilities. GDPR art. 28, paragraph 3, point c.
- ▶ To avoid loss, damage, theft or compromise of assets and disruptions in the organization. GDPR art. 28, paragraph 3, point c.

Control Activity	Test performed by BDO	Result of test
<b>Physical perimeter safety guarding</b> <ul style="list-style-type: none"> <li>▶ The established physical perimeter safety guarding is in agreement with the adopted security requirements.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's procedures for access control and escorted access to locations.</p> <p>We have inspected the physical perimeter safeguarding relating to office buildings.</p> <p>We observed, by random sampling, the handling of guest cards and we inspected the documentation of the selected samples.</p>	No deviations identified.
<b>Physical access control</b> <ul style="list-style-type: none"> <li>▶ Access controls have been established which guard against the probability of unauthorised physical access to, damage or interruption of GlobalConnect's premises and information - including ensuring that only authorised persons have access.</li> <li>▶ Activities are recorded in the access control system OMC.</li> <li>▶ Half-yearly review has been made of external access cards that have not been used within the last six months.</li> <li>▶ Half-yearly review has been made of internal access cards that have not been used within the last six months</li> <li>▶ Test control of selected access points to ensure that the right persons have the right accesses.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's procedures for access control and escorted access to locations and procedure for access control in connection with employment and departure of employees.</p> <p>We observed that the employees' physical access rights are granted on the basis of a work-related need, and that the management of these access rights is made in OMC. We have inspected documentation in this respect.</p> <p>We observed procedure for escorted access and inspected documentation in this respect in Service Management System by random sampling.</p> <p>We have observed procedure for customers' and suppliers' access, including access as a guest or access to administrative areas</p>	No deviations identified.

A.11: Physical and environmental security		
<p><b>Control Objective</b></p> <ul style="list-style-type: none"> <li>▶ <i>To prevent unauthorized physical access to, and damage/disruption of the organization's information and personal data, including information- and personal data processing facilities. GDPR art. 28, paragraph 3, point c.</i></li> <li>▶ <i>To avoid loss, damage, theft or compromise of assets and disruptions in the organization. GDPR art. 28, paragraph 3, point c.</i></li> </ul>		
Control Activity	Test performed by BDO	Result of test
	<p>We have inspected selected creations and closing down of customers' and suppliers' access. We have inspected extracts from the access control systems. We have observed the established access controls.</p> <p>We have inspected GlobalConnect's half-yearly review of external and internal access cards, which have not been used within the last six months, and the test control of access points.</p>	

## A.12: Operations security

### Control Objective

- ▶ To ensure proper and safe operation of information and data processing facilities. GDPR Art. 25, Art. 28, paragraph 3, point c.
- ▶ To ensure that information and personal data, including information and data processing facilities are protected against malware. GDPR Art. 28, paragraph 3, point c.
- ▶ To protect against data loss. GDPR Art. 28, paragraph 3, point c.
- ▶ To record events and provide evidence. GDPR Art. 33, paragraph 2.
- ▶ To ensure the integrity of operating systems. GDPR Art. 28, paragraph 3, point c.
- ▶ To prevent technical vulnerabilities being exploited. GDPR Art. 28, paragraph 3, point c.
- ▶ To minimize the impact of audit activities on operating systems. GDPR Art. 28, paragraph 1.

Control Activity	Test performed by BDO	Result of test
<b>Documented operating procedures</b> <ul style="list-style-type: none"> <li>▶ GlobalConnect has implemented formal operating procedures, which are available to all users having a function-related need for insight.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected Service Management System and inspected operating procedures and Knowledge Base, which is available to relevant users.</p> <p>We observed that operating manuals are prepared for the individual customers, and we observed, by random sampling, that they exist and are available to relevant users.</p>	No deviations identified.
<b>Change management</b> <ul style="list-style-type: none"> <li>▶ All changes to systems are managed and subject to the common change management process. Changes and management hereof are documented in Service Management System, in which the necessary approvals are registered.</li> <li>▶ Each change is subject to risk assessment and prioritised.</li> <li>▶ Customers are warned before the change work is commenced to ensure least possible inconvenience for the customers.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's procedures for Patch Management and for Change Management.</p> <p>We observed by random sampling for selected customers that patch management has been for these customers.</p> <p>We observed that risk assessment and prioritisation are made of the individual changes, and that a monitoring system is used which sends an alarm if critical systems are not operating.</p> <p>We observed that the planned work is created and managed in Service Management System, including warning of affected customers, follow up on work started and documentation of changes made.</p> <p>We have, by random sampling, inspected documentation for Change Management and Patch Management tasks performed in 2019.</p>	No deviations identified.



## A.12: Operations security

### Control Objective

- ▶ To ensure proper and safe operation of information and data processing facilities. GDPR Art. 25, Art. 28, paragraph 3, point c.
- ▶ To ensure that information and personal data, including information and data processing facilities are protected against malware. GDPR Art. 28, paragraph 3, point c.
- ▶ To protect against data loss. GDPR Art. 28, paragraph 3, point c.
- ▶ To record events and provide evidence. GDPR Art. 33, paragraph 2.
- ▶ To ensure the integrity of operating systems. GDPR Art. 28, paragraph 3, point c.
- ▶ To prevent technical vulnerabilities being exploited. GDPR Art. 28, paragraph 3, point c.
- ▶ To minimize the impact of audit activities on operating systems. GDPR Art. 28, paragraph 1.

Control Activity	Test performed by BDO	Result of test
<b>Capacity management</b> <ul style="list-style-type: none"> <li>▶ Monitoring and registration of customers' IT environment has been established for the customers who require management of the capacity to prevent system's break-down.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's procedures for Capacity Management.</p> <p>We have observed the set-up of the monitoring system, which sends an alarm when the determined maximum allowable value for unused capacity has been reached.</p> <p>We have inspected documentation, by random sampling, for capacity adjustments and changes made.</p>	No deviations identified.
<b>Separation of development, test and operation environments</b> <ul style="list-style-type: none"> <li>▶ GlobalConnect has separated IT environments into development, test and operating environments for the customers who require this.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's segmentation of IT environments and observed that they can be separated into development, test and operating environments.</p> <p>We have observed and inspected, by random sampling, that development, test and operating environments have been created for the customers who require this.</p>	No deviations identified.
<b>Controls against malware</b> <ul style="list-style-type: none"> <li>▶ All relevant entities in GlobalConnect's infrastructure are updated with approved malware software.</li> <li>▶ Malware software is updated with the most recent version (signature file).</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's procedure for antivirus program.</p>	No deviations identified.

## A.12: Operations security

### Control Objective

- ▶ To ensure proper and safe operation of information and data processing facilities. GDPR Art. 25, Art. 28, paragraph 3, point c.
- ▶ To ensure that information and personal data, including information and data processing facilities are protected against malware. GDPR Art. 28, paragraph 3, point c.
- ▶ To protect against data loss. GDPR Art. 28, paragraph 3, point c.
- ▶ To record events and provide evidence. GDPR Art. 33, paragraph 2.
- ▶ To ensure the integrity of operating systems. GDPR Art. 28, paragraph 3, point c.
- ▶ To prevent technical vulnerabilities being exploited. GDPR Art. 28, paragraph 3, point c.
- ▶ To minimize the impact of audit activities on operating systems. GDPR Art. 28, paragraph 1.

Control Activity	Test performed by BDO	Result of test
	<p>We were informed that it is not possible to have a server without having an antivirus program installed hereon. We have observed, by random sampling, that antivirus program is installed on the customer's servers.</p> <p>We observed that GlobalConnect's uses a logging and monitoring system which sends alarms at different stages to ensure that the antivirus program is operating and is updated and that the alarms are responded to.</p>	
<p><b>Backup of information - customers' data</b></p> <ul style="list-style-type: none"> <li>▶ Backup of data is taken for all customers with backup agreements, some via sub-processors and other internally in GlobalConnect.</li> <li>▶ Restore tests are carried out for customers with restore agreements according to the agreements.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's procedure for Managed TSM Backup and for Backup Restore Cloud Drift.</p> <p>We observed that GlobalConnect verifies backups and follows the procedure for managing of errors in the backups taken.</p> <p>We observed that the GlobalConnect has obtained and reviewed independent auditor's ISAE 3402 type 2 report for the period from 1 October 2018 to 30 September 2019 relating to technical and organisational security measures relating to the operation of Cloud Backup services.</p> <p>We were informed that GlobalConnect carries out restore test of data from backup if it is shown as a requirement in the agreement with the customer.</p> <p>We have randomly inspected documentation for restore test performed. We observed that restore test has been made and reported to the customer in accordance with the agreement.</p>	No deviations identified.

## A.12: Operations security

### Control Objective

- ▶ To ensure proper and safe operation of information and data processing facilities. GDPR Art. 25, Art. 28, paragraph 3, point c.
- ▶ To ensure that information and personal data, including information and data processing facilities are protected against malware. GDPR Art. 28, paragraph 3, point c.
- ▶ To protect against data loss. GDPR Art. 28, paragraph 3, point c.
- ▶ To record events and provide evidence. GDPR Art. 33, paragraph 2.
- ▶ To ensure the integrity of operating systems. GDPR Art. 28, paragraph 3, point c.
- ▶ To prevent technical vulnerabilities being exploited. GDPR Art. 28, paragraph 3, point c.
- ▶ To minimize the impact of audit activities on operating systems. GDPR Art. 28, paragraph 1.

Control Activity	Test performed by BDO	Result of test
<b>Incident logging</b> <ul style="list-style-type: none"> <li>▶ Recording and managing of all relevant incidents has been established.</li> <li>▶ Monitoring of customers' servers has been established for the purpose of accessibility and systems errors.</li> <li>▶ All incidents are logged in the Service Management System.</li> <li>▶ Any incidents concerning personal data leaks or suspicion of leaks are marked separately in order to sort these cases from other incidents.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected the procedure for Major Incident Management and for Incident Management for Outsourcing services.</p> <p>We have observed Incident Management System, and how Incidents are recorded.</p> <p>We inspected documentation of randomly selected incidents from list of all incidents recorded in 2019.</p> <p>We observed monitoring system and how the monitoring is set up to ensure accessibility and prevent potential systems errors or that services stop.</p> <p>We have inspected GlobalConnect's operating procedure for handling of incidents and on review of GlobalConnect's Service Management System we observed that all incidents are logged in their Service Management System.</p> <p>We observed how GlobalConnect records breach of the personal data security in the Service Management System.</p>	<p>We found that it is not possible for GlobalConnect to mark incidents concerning personal data leaks or suspicion of leaks separately in the Service Management System.</p> <p>Instead every incident concerning personal data leaks or suspicion of leaks are directed to the responsible department in GlobalConnect in the Service Management System.</p> <p>No other deviations identified.</p>
<b>Administrator and operator logs</b> <ul style="list-style-type: none"> <li>▶ Procedures are implemented to ensure that all activities performed by systems administrator or employees with administrative rights are recorded.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected the procedure for logging.</p> <p>We observed that monitoring and logging of activities performed by systems administrator or employees with administrative rights are recorded and date and time-stamped.</p>	<p>No deviations identified.</p>

## A.12: Operations security

### Control Objective

- ▶ To ensure proper and safe operation of information and data processing facilities. GDPR Art. 25, Art. 28, paragraph 3, point c.
- ▶ To ensure that information and personal data, including information and data processing facilities are protected against malware. GDPR Art. 28, paragraph 3, point c.
- ▶ To protect against data loss. GDPR Art. 28, paragraph 3, point c.
- ▶ To record events and provide evidence. GDPR Art. 33, paragraph 2.
- ▶ To ensure the integrity of operating systems. GDPR Art. 28, paragraph 3, point c.
- ▶ To prevent technical vulnerabilities being exploited. GDPR Art. 28, paragraph 3, point c.
- ▶ To minimize the impact of audit activities on operating systems. GDPR Art. 28, paragraph 1.

Control Activity	Test performed by BDO	Result of test
	<p>We observed that a system is used for managing of alarms and notifications which ensures a prompt overview and that the most important alarms are managed first.</p> <p>We observed that this logging applies to both GlobalConnect and GlobalConnect's customers.</p>	
<b>Time synchronisation</b> <ul style="list-style-type: none"> <li>▶ Infrastructure components have been implemented which are time synchronised up to centralised NTP servers.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected the set-up of time synchronisation and observed that the time synchronization has been set up to centralised NTP servers.</p>	No deviations identified.

### A.13: Communications security

#### Control Objective

- ▶ To ensure protection of network information and personal data and supportive information and personal data processing facilities. GDPR art. 28, paragraph 3, point c.
- ▶ To maintain information security and data protection when transferring internally in an organisation and to an external entity. GDPR art. 28, paragraph 3, point c.

Control Activity	Test performed by BDO	Result of test
<p><b>Policies and procedures for transfer of information</b></p> <ul style="list-style-type: none"> <li>▶ Formal business procedures have been implemented to safeguard internal and external transfers of confidential or sensitive information or data, where required.</li> <li>▶ Remote access has been established to GlobalConnect's systems for customers requiring this. The access is either through public networks, protected by VPN or MPLS and firewall.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected procedure and guide to set-up of VPN and encryption for creation of new customers and set-up of firewalls.</p> <p>We have inspected guides and Knowledge Details relating to management of certificates which safeguard the confidentiality of external transfers, including creation and renewal of certificates.</p> <p>We have inspected list of customers who have made an agreement for set-up of certificates and observed these by random sampling.</p>	<p>No deviations identified.</p>

## A.14: System acquisition, development and maintenance of systems

Control Objective		
<ul style="list-style-type: none"> <li>▶ To ensure that information security and data protection is an integral part of information systems throughout the life cycle. This also includes the requirements for information systems that provide public network services. GDPR art. 25.</li> <li>▶ To ensure that information security and data protection is organised and implemented within the information systems development life cycle. GDPR art. 25.</li> <li>▶ To ensure the protection of data used for testing. GDPR art. 25.</li> </ul>		
Control Activity	Test performed by BDO	Result of test
<b>Technical review of applications after changes to operating platforms</b> <ul style="list-style-type: none"> <li>▶ Formal processes and procedures have been implemented for all changes made in the company's own IT environment.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected the Change Management procedure manual.</p> <p>We observed that there is priority level for Change Managements, according to which delegation is made to the relevant employees. We have inspected matrix for assessment of type of change and risks.</p> <p>We have inspected, by random sampling, documentation for changes made from Service Management System.</p>	No deviations identified.
<b>Software installation in operating systems</b> <ul style="list-style-type: none"> <li>▶ Formal business routines and procedures for implementation of software in own and the customers' environments.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's procedures for Change Management and Patch Management for implementation of software.</p> <p>We have inspected, by random sampling, the documentation for management of software in own and the customers' environments in 2019.</p>	No deviations identified.
<b>Management of technical vulnerabilities</b> <ul style="list-style-type: none"> <li>▶ Formal processes and procedures (Patch Management) have been implemented for security updates of operating systems.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's procedures for Patch Management.</p> <p>We observed that a risk assessment and prioritisation of the individual changes are made, and that a monitoring system sends an alarm if critical systems are not operating.</p>	No deviations identified.

### A.14: System acquisition, development and maintenance of systems

#### Control Objective

- ▶ *To ensure that information security and data protection is an integral part of information systems throughout the life cycle. This also includes the requirements for information systems that provide public network services. GDPR art. 25.*
- ▶ *To ensure that information security and data protection is organised and implemented within the information systems development life cycle. GDPR art. 25.*
- ▶ *To ensure the protection of data used for testing. GDPR art. 25.*

Control Activity	Test performed by BDO	Result of test
	<p>We observed that planned work is created and managed in Service Management System, including warning of affected customers, follow-up on work started and documentation of changes made.</p> <p>We have randomly selected customers from the list of all GlobalConnect's customers and examined whether security updates (Patch Management) are made in 2019.</p>	

A.15: Supplier relationships		
<b>Control Objective</b> ▶ To ensure protection of the organization's assets and personal data that suppliers have access to. GDPR Art. 28, paragraph 2, Art. 28, paragraph 3, point d, Art. 28, paragraph 4. ▶ To maintain an agreed level of information security, data protection and delivery of services under the supplier agreements. GDPR Art. 28, paragraph 2, Art. 28, paragraph 3, point d, Art. 28, paragraph 4.		
Control Activity	Test performed by BDO	Result of test
<b>Information security handbook for supplier relationships</b> ▶ GlobalConnect's sub-processors are familiar with the contents of our information security manual, which is handed out together with new agreements or changes to existing agreements.	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected the data processing agreement between GlobalConnect and Frontsafe A/S. We have observed that GlobalConnect has not entered into new agreements with any sub-processors.</p> <p>We were not able to verify the procedure regarding handing out the information security manual together with new agreements or changes to existing agreements, because GlobalConnect has not entered into any new agreements or made changes to existing agreements with sub-processors.</p>	No deviations identified.
<b>Management of security of service organisation agreements</b> ▶ All relevant suppliers have signed a NDA with GlobalConnect and are familiar with the content of our information security manual.	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected Service Level Agreement from Frontsafe A/S relating to Cloud Backup services.</p> <p>We have inspected non-disclosure agreement from G4S.</p> <p>We were not able to verify the effectiveness in 2019 because no agreements were made with suppliers requiring non-disclosure agreements.</p>	No deviations identified.
<b>Addressing personal data protection for supplier relationships</b> ▶ In the use of sub-processors, GlobalConnect makes a data processing agreement which imposes the same data protection obligations on the sub-processor as those imposed on GlobalConnect. ▶ GlobalConnect uses FrontSafe as a sub-processor for backup solutions, who provides an annual ISAE 3402 auditor's report.	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected the data processor agreement between Globalconnect and Frontsafe A/S. We observed that it is Frontsafe A/S' template that is used.</p> <p>We were informed that GlobalConnect reviews the data processing agreement with Frontsafe A/S before entering the agreement to ensure that it imposes the same data protection obligations as imposed on GlobalConnect.</p>	No deviations identified.



## A.15: Supplier relationships

### Control Objective

- ▶ To ensure protection of the organization's assets and personal data that suppliers have access to. GDPR Art. 28, paragraph 2, Art. 28, paragraph 3, point d, Art. 28, paragraph 4.
- ▶ To maintain an agreed level of information security, data protection and delivery of services under the supplier agreements. GDPR Art. 28, paragraph 2, Art. 28, paragraph 3, point d, Art. 28, paragraph 4.

Control Activity	Test performed by BDO	Result of test
	<p>We observed that information on the use of sub-processors is listed in relevant data processor agreements with the customers.</p> <p>We observed that GlobalConnect has obtained an annual ISAE 3402 auditor's report from the sub-processor Frontsafe A/S.</p>	
<p><b>Control with service organisations</b></p> <ul style="list-style-type: none"> <li>▶ Business procedures have been established to ensure supervision of GlobalConnect's implemented controls in the form of obtaining an ISAE 3402 auditor's report.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected Service Level Agreement from Frontsafe A/S relating to Cloud Backup services.</p> <p>We observed that the GlobalConnect has obtained and reviewed independent auditor's ISAE 3402 type 2 report for the period from 1 October 2018 to 30 September 2019 relating to technical and organisational security measures relating to the operation of Cloud Backup services.</p> <p>We have inspected the above mentioned ISAE 3402 report.</p>	No deviations identified.

## A.16: Information security incident management

### Control Objective

- ▶ To ensure a uniform and effective method of managing information security breaches and personal data breaches, including communication on security incidents and weaknesses. GDPR Art. 33, paragraph 2.

Control Activity	Test performed by BDO	Result of test
<p><b>Handling of information security incidents</b></p> <ul style="list-style-type: none"> <li>▶ All security incidents are managed in Service Management System and in accordance with established procedures.</li> <li>▶ GlobalConnect has implemented procedures for documentation of all personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.</li> <li>▶ Guidelines to reporting information security incidents have been implemented and communicated to the employees in QRC, who are responsible for data protection in GlobalConnect.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's information security policy and information security rules, and procedures for management of security incidents.</p> <p>We have inspected procedures for Major Incident Management and Incident Management and operating procedure for management of security incidents.</p> <p>We observed that all security incidents received are recorded in Service management System, where they are assessed with respect to impact and severity which together give a prioritisation of security incidents. We also observed that an explanatory text is added to the security incident so that relevant employees can make a further assessment/prioritisation hereof.</p> <p>We have inspected GlobalConnect's procedure for handling of incidents, internal procedure for reporting of personal data breaches to the responsible department in GlobalConnect and template for registration of information regarding personal data breaches.</p> <p>We have observed that all personal data breaches are recorded in the Service Management System and the employee, who detects or receives an inquiry about a personal data breach, informs the responsible person in GlobalConnect.</p> <p>We observed that the employees at GlobalConnect are informed about the guidelines regarding personal data breaches.</p> <p>We observed that GlobalConnect has had a suspicion of a personal data breach and that the internal procedure regarding handling of incidents was followed. The result of a further investigation of the breach was that it was not a personal data breach.</p>	<p>No deviations identified.</p>

A.16: Information security incident management		
<b>Control Objective</b> ▶ To ensure a uniform and effective method of managing information security breaches and personal data breaches, including communication on security incidents and weaknesses. GDPR Art. 33, paragraph 2.		
Control Activity	Test performed by BDO	Result of test
	We were not able to verify the procedures regarding documentation of personal data breach, because there have not been any personal data breaches.	
<b>Reporting of information security incidents</b> <ul style="list-style-type: none"> <li>▶ Processes and procedures have been established for handling of security incidents to ensure a uniform and effective method of managing information security incidents, including communication of security incidents and weaknesses which are documented in Service Management System.</li> <li>▶ Processes and procedures have been established to ensure recording and handling of security incidents by the right employee.</li> <li>▶ Procedures have been implemented based on the data processing agreements with our customers to ensure handling of personal data and responding to security incidents within the agreed time frames.</li> <li>▶ GlobalConnect has implemented a template for notification of the personal data breach to the data controller, which ensures that it contains the necessary information.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's information security policy and information security rules, and procedures for management of security incidents.</p> <p>We have inspected procedures for Major Incident Management and Incident Management and operating procedure for management of security incidents.</p> <p>We observed that processes and procedures have been established for handling of security incidents to ensure a uniform treatment hereof, see control activity for information security incident management.</p> <p>We observed that security incidents and breaches are assessed and hereafter assigned to an employee to ensure that the right employee manages the incident or the breach.</p> <p>We observed that the customer is informed of security incidents and that, in case of major security incidents, a written report is subsequently sent to the customer.</p> <p>We have inspected GlobalConnect's template for data processing agreement and procedures for handling of personal data breaches and observed that these are aligned.</p> <p>We have inspected randomly selected data processing agreements entered into with customers and observed that GlobalConnect's procedures for notifying the customer of a personal data breach are in accordance with entered data processing agreements with customers.</p>	No deviations identified.

## A.16: Information security incident management

### Control Objective

- ▶ To ensure a uniform and effective method of managing information security breaches and personal data breaches, including communication on security incidents and weaknesses. GDPR Art. 33, paragraph 2.

Control Activity	Test performed by BDO	Result of test
	<p>We have inspected GlobalConnect's template of notification of the customers and observed that it contains all necessary information about the personal data breach.</p> <p>We were not able to verify the procedures regarding documentation of personal data breach, because there have not been any personal data breaches.</p>	
<h3>Learning from information security incidents</h3> <ul style="list-style-type: none"> <li>▶ It is assessed if new measures need to be implemented to avoid future information security incidents.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have observed GlobalConnect's procedures for handling of personal data breaches including measurement of the breach to learn from and avoid future personal data breaches.</p> <p>We were not able to verify the procedures regarding subsequent handling of personal data breaches because there have not been any personal data breaches.</p>	No deviations identified.

### A.17: Information security aspects of disaster recovery, contingency and restore management

#### Control Objective

- ▶ To ensure that information security- and data protection continuity is rooted in the organization's management systems for emergency and re-establishment. GDPR Art. 28, paragraph 3, point c.
- ▶ To ensure accessibility of information- and personal data processing facilities. GDPR Art. 28, paragraph 3, point c.

Control Activity	Test performed by BDO	Result of test
<b>Implementation of information security continuity</b> <ul style="list-style-type: none"> <li>▶ Contingency plans are prepared for relevant functions to ensure business continuance in connection with security incidents.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected contingency plans for 2019 for relevant functions to ensure business continuance in connection with security incidents.</p> <p>We observed that the list includes plans for performance of test of contingency plans for different scenarios.</p>	No deviations identified.
<b>Verify, review and evaluate the information security continuity</b> <ul style="list-style-type: none"> <li>▶ GlobalConnect has established periodical testing of contingency plans for the purpose of ensuring that the contingency plans are up-to-date and effective in critical situations.</li> <li>▶ Contingency tests are documented by reports from testing.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We inspected documentation for 2 planned desk tests of 2 contingency plans for relevant areas.</p> <p>We observed that GlobalConnect has complete tests according to the planned scenarios by performing desk tests of contingency plans.</p> <p>Based on test, GlobalConnect assesses that the contingency plans should be adjusted.</p>	No deviations identified.
<b>Availability of information processing facilities</b> <ul style="list-style-type: none"> <li>▶ Redundancy has been established in relevant systems for the customers requiring this to meet availability requirements.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected agreement and scenario for failover and operational test in relation to test of redundant systems providing power to racks, Storage Controller, firewalls and switches.</p> <p>We inspected documentation and observed that GlobalConnect has carried out and reported redundancy tests in 2019 for the customers requesting tests.</p>	No deviations identified.

A.18: Compliance		
<b>Control Objective</b> <ul style="list-style-type: none"> <li>▶ To prevent violations of statutory, regulatory or contractual requirements in relation to information security and other security requirements. GDPR Art. 25, Art. 28, paragraph 2, Art. 28, paragraph 3, point a, Art. 28, paragraph 3, point e, Art. 28, paragraph 3, point g, Art. 28, paragraph 3, point h, Art. 28, paragraph 3, point f, Art. 28, paragraph 10, Art. 29, Art. 32, paragraph 4, Art. 33, paragraph 2.</li> <li>▶ To ensure that information security and data protection is implemented and run in accordance with the organization's policies and procedures. GDPR Art. 28, paragraph 1.</li> </ul>		
Control Activity	Test performed by BDO	Result of test
<b>Identification of applicable legislation and contractual requirements</b> <ul style="list-style-type: none"> <li>▶ GlobalConnect has identified all relevant legal and public authority requirement.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected procedure for compliance with legal and public authority requirements.</p> <p>We have inspected GlobalConnect's documentation for review of legal and public authority requirements and observed that relevant legislation have been reviewed, documented and approved by Management. This was most recently carried out in April 2019.</p>	<p>We found that GlobalConnect's documentation for review of legislative and government requirements does not include the following legislative and government requirements:</p> <ol style="list-style-type: none"> <li>1. The General Data Protection Regulation and the Data Protection Act</li> <li>2. Executive Orders pursuant to the Act of Network and Information Security</li> </ol> <p>No other deviations identified.</p>
<b>Privacy and protection of personally identifiable information</b> <ul style="list-style-type: none"> <li>▶ GlobalConnect has procedures for making written, electronic data processing agreements, including template for data processing agreement in accordance with the services provided.</li> <li>▶ Data processing agreements have been entered with the relevant customers and stored electronically.</li> <li>▶ Data processing agreements include information on the use of sub-processors.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's procedures and template for entering into data processing agreements with customers. We have observed that the template for the data processing agreement complies with the requirements relating to the content of a data processing agreement in accordance with General Data Protection Regulation article 28(3), and that it includes information on the use of sub-processors.</p> <p>We have inspected randomly selected data processing agreements entered into with customers and observed that the data processing agreements are in accordance with the service provided, are stored electronically and include information on the use of sub-processors.</p>	<p>We found that GlobalConnect has not signed 1 out of 4 randomly selected data processing agreements.</p> <p>No other deviations identified.</p>
<b>Instruction for processing of personal data</b> <ul style="list-style-type: none"> <li>▶ GlobalConnect stores and processes personal data according to the customer's instruction for the customers who have made a data processing agreement with us.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's procedures and template for entering into data processing agreements with customers.</p>	<p>No deviations identified.</p>

## A.18: Compliance

### Control Objective

- ▶ To prevent violations of statutory, regulatory or contractual requirements in relation to information security and other security requirements. GDPR Art. 25, Art. 28, paragraph 2, Art. 28, paragraph 3, point a, Art. 28, paragraph 3, point e, Art. 28, paragraph 3, point g, Art. 28, paragraph 3, point h, Art. 28, paragraph 3, point f, Art. 28, paragraph 10, Art. 29, Art. 32, paragraph 4, Art. 33, paragraph 2.
- ▶ To ensure that information security and data protection is implemented and run in accordance with the organization's policies and procedures. GDPR Art. 28, paragraph 1.

Control Activity	Test performed by BDO	Result of test
<ul style="list-style-type: none"> <li>▶ Data processing agreements provide terms to the effect that the data controller must be informed of instructions which are not compliant with legislation.</li> </ul>	<p>We have observed that GlobalConnect stores and processes personal data according to the customer's instruction and inform the customers if instructions in the data processing agreements are not compliant with legislation.</p> <p>We have inspected randomly selected data processing agreements entered into with customers and observed that GlobalConnect processes customer data in accordance with the instruction from the customers and must inform the customers if instructions are not compliant with legislation.</p>	
<h3>Assistance to the data controller</h3> <ul style="list-style-type: none"> <li>▶ GlobalConnect has an obligation according to the data processing agreements to assist the customers in relation to requests for exercising of the data subjects' rights.</li> <li>▶ GlobalConnect has an obligation according to the data processing agreements to assist the customers with their obligations according to articles 32 to 36.</li> <li>▶ GlobalConnect has an obligation according to the data processing agreements to obtain an ISAE 3000 report annually for the purpose of the customer's inspection of GlobalConnect.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's template for data processing agreements and observed that GlobalConnect has an obligation to assist the customer in relation to requests for exercising of the data subjects' rights, with their obligations according to article 32 to 36 and for the purpose of the customer's inspection of GlobalConnect.</p> <p>We have inspected GlobalConnect's procedure for requests relating to personal data and assistance to the customer. We have observed that GlobalConnect's procedures contain guidelines for assistance to the customer regarding requests for exercising of the data subjects' rights, with their obligations according to article 32 to 36 and for the purpose of the customer's inspection of GlobalConnect.</p> <p>We have inspected randomly selected data processing agreements entered into with customers and observed that GlobalConnect has an obligation to assist the customer in relation to requests for exercising of the data subjects' rights, assist accordingly to article 32 to 36 and for the purpose of the customer's inspection of GlobalConnect.</p>	No deviations identified.

A.18: Compliance		
<b>Control Objective</b> <ul style="list-style-type: none"> <li>▶ To prevent violations of statutory, regulatory or contractual requirements in relation to information security and other security requirements. GDPR Art. 25, Art. 28, paragraph 2, Art. 28, paragraph 3, point a, Art. 28, paragraph 3, point e, Art. 28, paragraph 3, point g, Art. 28, paragraph 3, point h, Art. 28, paragraph 3, point f, Art. 28, paragraph 10, Art. 29, Art. 32, paragraph 4, Art. 33, paragraph 2.</li> <li>▶ To ensure that information security and data protection is implemented and run in accordance with the organization's policies and procedures. GDPR Art. 28, paragraph 1.</li> </ul>		
Control Activity	Test performed by BDO	Result of test
	We were not able to verify GlobalConnect's handling of assistance to the customer because there have not been any requests for this purpose.	
<b>Deletion and return of customers data</b> <ul style="list-style-type: none"> <li>▶ Policies have been implemented to ensure protection of customer's confidential and sensitive information when off-boarding a customer.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected GlobalConnect's procedure for deletion and return of the customer's data and observed that GlobalConnect only processes personal data according to instructions from the customer, including deletion and return of data when the agreement ends.</p> <p>We were not able to verify GlobalConnect's procedure for deletion and return of the customer's data when the agreement ends, because there were no requests for this purpose.</p>	No deviations identified.
<b>Independent review of controls</b> <ul style="list-style-type: none"> <li>▶ Compliance with the EU General Data Protection Regulation (GDPR) is verified by obtaining an annual audit report from an independent auditor demonstrating compliance.</li> <li>▶ GC-OS is ISO9001 and ISO27001 certified. As a part hereof, procedures are drawn of for an annual reassessment and approval of descriptions of underlying policies, processes and procedures.</li> </ul>	<p>We have interviewed relevant personnel at GlobalConnect.</p> <p>We have inspected randomly selected data processing agreements entered into with customers and observed that GlobalConnect has an obligation to assist the customer in relation to their obligations to supervise GlobalConnect.</p> <p>We have prepared this ISAE 3000 report for the purpose of GlobalConnect's obligations in this respect.</p> <p>We have inspected the ISO9001:2015 certificate relating to Dedicated IT Outsourcing and Infrastructure Operations applicable for the period from period from 22 August 2018 to 12 August 2021.</p> <p>We have inspected the ISO27001:2013 certificate relating to Dedicated IT Outsourcing and Infrastructure Operations According to Statement of Applicability applicable for the period from 19 August 2018 to 12 August 2021.</p>	No deviations identified.



## A.18: Compliance

### Control Objective

- ▶ *To prevent violations of statutory, regulatory or contractual requirements in relation to information security and other security requirements. GDPR Art. 25, Art. 28, paragraph 2, Art. 28, paragraph 3, point a, Art. 28, paragraph 3, point e, Art. 28, paragraph 3, point g, Art. 28, paragraph 3, point h, Art. 28, paragraph 3, point f, Art. 28, paragraph 10, Art. 29, Art. 32, paragraph 4, Art. 33, paragraph 2.*
- ▶ *To ensure that information security and data protection is implemented and run in accordance with the organization's policies and procedures. GDPR Art. 28, paragraph 1.*

Control Activity	Test performed by BDO	Result of test
	<p>We inspected GlobalConnect's annual wheel for examination of information security policies, information security rules, and information security manual.</p> <p>We observed that the annual wheel is complied with, and that the information security policy is examined and reassessed. We inspected relevant documentation.</p>	

## SUPPLEMENTARY INFORMATION FROM GLOBALCONNECT A/S

### 1. Information on Ransomware attack in November 2019

On Saturday, 23 November 2019, at 22.00, the in-house IT department found that several units were not accessible. The incident was hereafter escalated internally in the organisation. After analysing the situation, it was clear that GlobalConnect A/S was attacked by Ransomware (Ransom.Sodinokibi) on the internal administrative systems. The ransomware spread through the SMB protocol locally on the office domain via certain, hacked AD identification information with administrative rights. Within seconds, 100+ servers were infected. All GlobalConnect A/S' production domains were quickly isolated, so that the attack was contained to include only our office domains. GlobalConnect A/S' internal systems were subsequently fully restored after the incident.

### 2. GlobalConnect A/S' action plan

Action plan		
Control activity	Result of test	Initiative
Risk assessment	We have observed that the risk assessment does not include assessment of risks and consequences for the data subjects.	The risk assessment will include consequences to the data subject, if it makes sense in the data processing of the customers data
A.5: Information security policies  Review of policies for information security	We found that the information security policy has not been approved by the Senior Management's signing in 2019.	Management's signatures were not available at the time of our audit. The signatures have been obtained subsequently.
	We found that GlobalConnect's Personal Data Policy and data classification policy has not been reviewed and updated in 2019.	The data classification policy has been reviewed in 2019 but here has not been any changes to the policy, so therefore isn't it updated
A.6: Organisation of information security  Remote workplaces and mobile equipment	We found that there are 5 units for which status for antimalware is "off".	When the 5 units have Antimalware status "off" in the report, it is not because they are off but because there is an issue with that part of Bitdefender Endpoint Security, which is examined further by the in-house IT department.
A.7: Staff security  During employment	We found that 2 out of 15 employees have not confirmed by their signature that they have read and accepted the information security policy and manual.	To ensure robust business procedures GlobalConnect performs at present regular adjustment of the internal processes which, among others, have been of importance for the onboarding process, including the date on which the relevant documents are signed in connection with employments. The signatures were obtained subsequently.
A.9: Access management  Granting, adjustment and disabling of access rights	We found that two resigned employees continue to have access to Active Directory.	The relevant employees were granted access as consultants in addition to their normal work-related accounts. Both accounts were closed subsequently.
A.9: Access management  Management of privileged access rights	We found that there is no documentation that 24 enterprise-admins, 60 domain_admins and 94 builtin_admins have these rights based on functional needs.	This domain is being wound up and is not important for production purposes but is solely maintained out of regard to internal administrative systems. The domain will be closed during 2020.

Action plan		
Control activity	Result of test	Initiative
A.12: Operations security  Incident logging	We found that it is not possible for GlobalConnect to mark incidents concerning personal data leaks or suspicion of leaks separately in the Service Management System. Instead every incident concerning personal data leaks or suspicion of leaks are directed to the responsible department in GlobalConnect in the Service Management System.	We have no indication of breaches on personal data, instead we mark incidents of that character as Security Incidents. Our procedures for handling of Security Incidents tells, that every incident have to be reported to the CISO, who also are the company's DPO.
A.18: Compliance  Identification of applicable legislation and contractual requirements	We found that GlobalConnect's documentation for review of legislative and government requirements does not include the following legislative and government requirements:  1. The General Data Protection Regulation and the Data Protection Act  3. Executive Orders pursuant to the Act of Network and Information Security	"Law on Compliance sheet" is updated with the described legislative and government requirements.
A.18: Compliance  Privacy and protection of personally identifiable information	We found that GlobalConnect has not signed 1 out of 4 randomly selected data processing agreements.	The data processing agreements is our customers instruction to us, so if we have signed it or not doesn't matter at all.

**BDO STATSATORISERET  
REVISIONSAKTIESELSKAB**

HAVNEHOLMEN 29  
1561 KØBENHAVN V

CVR NO. 20 22 26 70

*BDO Statsautoriseret revisionsaktieselskab, a Danish limited liability company, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO in Denmark employs almost 1,200 people and the worldwide BDO network has more than 80,000 partners and staff in 160 countries.*

*Copyright - BDO Statsautoriseret revisionsaktieselskab, CVR No. 20 22 26 70.*

